On Generalizations of p-Adic Weierstrass Sigma and Zeta Functions

by

Clifford Blakestad

B.S., California Institute of Technology, 2011

A thesis submitted to the

Faculty of the Graduate School of the

University of Colorado in partial fulfillment

of the requirements for the degree of

Doctor of Philosophy

Department of Mathematics

2018

This thesis entitled:
On Generalizations of p-Adic Weierstrass Sigma and Zeta Functions
written by Clifford Blakestad
has been approved for the Department of Mathematics

Prof. David Grant

Prof. Jonathan Wise

Date ____________________

The final copy of this thesis has been examined by the signatories, and we find that both the content and the form meet acceptable presentation standards of scholarly work in the above mentioned discipline.

Blakestad, Clifford (Ph.D., Mathematics)

On Generalizations of p-Adic Weierstrass Sigma and Zeta Functions

Thesis directed by Prof. David Grant

We generalize a paper of Mazur and Tate on p-adic sigma functions attached to elliptic curves of ordinary reduction over a p-adic field.

We begin by generalizing the theory of division polynomials attached to an isogeny of elliptic curves, developed by Mazur and Tate, to isogenies of prinicipally polarized abelian varieties. As an application, we produce a notion of a p-adic sigma function attached to a prinicipally polarized abelian variety of good ordinary reduction over a complete non-archimedean field of residue characteristic p. Furthermore, we derive some the properties of the sigma function, many of which uniquely characterize the function.

Independently, a notion of a pair of p-adic Weierstrass zeta functions is produced for a smooth projective curve C of genus two with invertible Hasse–Witt matrix over a p-adically complete field of characteristic zero.

Using the explicit function theory afforded by Jacobians of genus two, general results about p-adic sigma functions are made more descriptive and the zeta functions on C are compared to the second logarithmic derivatives of the sigma function on the Jacobian of C.

Dedication

To the memory of Julius E. Johnson Jr.

Acknowledgements

My education benefited greatly from the kindness and accesibility of a great many of the faculty in the mathematics department at the University of Colorado Boulder. I will specifically mension three. I would especially like to thank David Grant for his willingness to guide such a stubborn student and entertain many hours of interesting conversation. I would like to thank Jonathan Wise for his willingness to answer my many questions and his general cheerfulness in discussing mathematics from his first week in Boulder until my last. I would like to thank Sebastian Casalaina-Martin for always making time to talk since I first arrived in Boulder.

Finally, I would like to thank my family. This thesis would not have happened without their endless encouragement and their focus on education.

Contents

Chapter

1 Introduction **1**

1.1 History . . . 2

1.1.1 Complex sigma and theta functions . . . 2

1.1.2 Algebraic theta functions . . . 5

1.1.3 p-Adic theories . . . 7

1.2 This thesis . . . 10

2 Sigma functions on abelian varieties **15**

2.1 Preliminaries on abelian varieties . . . 15

2.1.1 Abelian varieties . . . 15

2.1.2 Line bundles . . . 15

2.1.3 Models . . . 19

2.1.4 Ordinary reduction . . . 21

2.1.5 Group schemes . . . 21

2.1.6 Formal groups . . . 23

2.2 p-Adic sigma functions on abelian varieties . . . 24

2.2.1 Division polynomials . . . 26

2.2.2 Towers . . . 29

2.2.3 Sigma functions . . . 35

2.3 Properties of σ functions . . . 37

3 Weierstrass zeta functions on curves of genus two **48**

3.1 Preliminaries on curves 48

3.1.1 Hyperelliptic curves 49

3.2 Weierstrass zeta functions in genus two 50

3.2.1 Hasse-Witt matrices 51

3.2.2 Weierstrass zeta functions 54

3.2.3 Universal p-adic zeta functions 58

3.2.4 Appendix: t-expansions 59

4 Jacobians of curves of genus two **61**

4.1 Preliminaries on curves and Jacobians 61

4.1.1 Jacobians 61

4.1.2 Symmetric powers of curves 62

4.2 p-Adic Weierstrass sigma function in dimension two 70

4.3 p-Adic Weierstrass zeta functions in dimension two 73

4.4 Future work 78

Bibliography **80**

Chapter 1

Introduction

Beginning in the middle of the nineteenth century, theta functions have enjoyed a long history in the study of curves and abelian varieties. Even in the twentieth and into the twenty-first centuries, the line bundles they represent have played a central role in understanding the arithmetic and geometry of curves, abelian varieties, and their moduli spaces.

The classical theta functions were holomorphic functions on $\mathbb{C}^g$ which were quasiperiodic with respect to some lattice $\Lambda \subseteq \mathbb{C}^g$, i.e., for each λ in Λ, there is some complex constant c_λ and some linear function $f_\lambda : \mathbb{C}^g \to \mathbb{C}$ such that $\vartheta(z+\lambda) = c_\lambda e^{f_\lambda(z)}\vartheta(z)$ for all z in $\mathbb{C}^g$. A theta function $\vartheta(z)$ is said to be nondegenerate if it is not constant on the cosets of some nontrivial subspace $V \subseteq \mathbb{C}^g$. As every degenerate theta function is the pullback of a nondegenerate theta function on some quotient vector space, we will be primarily interested in studying nondegenerate theta functions. Some of the details of the classical theories are presented in the historical comments below. Geometrically speaking, a theta function can be thought of as an explicit trivialization of a section of a line bundle on the quotient $\mathbb{C}^g/\Lambda$. If the theta function is nondegerate, this quotient has the structure of an abelian variety.

From the above functional expression, one can see that if z_i is the i-th coordinate function on $\mathbb{C}^g$, then for each λ in Λ the function $\frac{d}{dz_i}\log\vartheta(z)$ satisfies $\frac{d}{dz_i}\log\vartheta(z+\lambda) = \eta_\lambda + \frac{d}{dz_i}\log\vartheta(z)$ where $\eta_\lambda = \frac{d}{dz_i}f_\lambda$ is a constant in z because $f_\lambda(z)$ is linear in z. Geometrically, the logarithmic derivatives of $\vartheta(z)$ with respect to all of the $\frac{d}{dz_i}$ can be thought of as giving a basis for the universal vectoral extension of the abelian variety $\mathbb{C}^g/\Lambda$.

Taking another derivative will kill off the constant η_λ so that $\frac{d}{dz_i}\frac{d}{dz_j}\log\vartheta(z)$ is invariant under translation by elements of Λ. Hence the second logarithmic derivatives of $\vartheta(z)$ (and all higher log-derivatives) descend to meromorphic functions on the abelian variety $\mathbb{C}^g/\Lambda$.

We see that $\vartheta(z)$ is some power series in $z_1,\ldots,z_g$ whose coefficients must somehow capture an enormous amout of data relating to the abelian variety $\mathbb{C}^g/\Lambda$. There is then hope that even over fields other than $\mathbb{C}$, one could attach power series ϑ to an abelian variety A which encodes the same geometric information about A. Indeed, general algebraic theories now exist and some of their details are mentioned below, but general rings lack notions of convergence so such a series is a purely formal consideration. In fields complete with respect to a non-archimedean absolute value, one can hope for additional benefit from producing a convergent power series ϑ. The goal of this thesis is to contribute to the theory of theta functions attached to curves and abelian varieties over such fields.

1.1 History

Sigma functions and the closely associated theta functions have a long history in algebraic geometry and number theory. We will briefly give an account of various parts of their theory as they apply to the study of abelian varieties to add some context for our results and to have the opportunity to discuss some of the ideas we generalize in this thesis.

1.1.1 Complex sigma and theta functions

The classical setting of sigma and theta functions is over the complex numbers.

1.1.1.1 Classical Weierstrass functions

Any elliptic curve over the complex numbers can be expressed as a complex torus, i.e., as $\mathbb{C}/\Lambda$ for a rank two lattice $\Lambda = \mathbb{Z}+\tau\mathbb{Z}$, for some τ in the upper half-plane (that is τ has a positive imaginary part). Back in the 1850s, Weierstrass wrote down three functions which have become fundamental in the study of elliptic curves

$$\wp(z) = \frac{1}{z^2} + \sum_{\substack{\lambda\in\Lambda \\ \lambda\neq 0}} \frac{1}{(z-\lambda)^2} - \frac{1}{\lambda^2}$$

$$\zeta(z) = \frac{1}{z} + \sum_{\substack{\lambda\in\Lambda \\ \lambda\neq 0}} \frac{1}{z-\lambda} + \frac{1}{\lambda} + \frac{z}{\lambda^2}$$

$$\sigma(z) = z \prod_{\substack{\lambda\in\Lambda \\ \lambda\neq 0}} \left(1 - \frac{z}{\lambda}\right) e^{\frac{z}{\lambda} + \frac{1}{2}\left(\frac{z}{\lambda}\right)^2}.$$

They have the differential relations

$$\frac{d}{dz}\log(\sigma(z)) = \zeta(z)$$

$$\frac{d}{dz}\zeta(z) = -\wp(z).$$

The function $\sigma(z)$ has simple zeroes on Λ and no other zeroes or poles, $\zeta(z)$ has simple poles with residue 1 on Λ with no other poles, and $\wp(z)$ has poles of order two (and residue 0) on Λ. The function $\wp(z)$ is periodic with respect to translation by Λ, while Liouville's theorem and the residue theorem imply that no functions with these properties of $\sigma(z)$ or $\zeta(z)$ could be periodic with respect to Λ.

Nevertheless, ζ and σ have simple functional equations under translation. We have

$$\zeta(z+\lambda) = \zeta(z) + \eta(\lambda)$$

where $\eta(\lambda)$ is $\mathbb{Z}$-linear in Λ and

$$\sigma(z+\lambda) = \pm\sigma(z)e^{\eta(\lambda)(z+\lambda)}$$

where the ± 1 depends on whether or not λ is in 2Λ.

The function $\wp'(z) = \frac{d}{dz}\wp(z)$ is also periodic with respect to Λ and satifies the equation

$$\left(\frac{1}{2}\wp'(z)\right)^2 = \wp(z)^3 + A\wp(z) + B$$

for complex numbers A, B (depending on τ). Then if E is the variety (set of solutions) associated to the curve $y^2 = x^3 + Ax + b$, we get a map $\mathbb{C} \to E$ taking $z \mapsto \left(\wp(z), \frac{1}{2}\wp'(z)\right)$ for z not in Λ, with Λ mapping to the point at infinity on the curve.

In more modern language, we see that $\wp(z)$ is a meromorphic function on $\mathbb{C}/\Lambda$ while $\sigma(z)$ describes a section of the line bundle on $\mathbb{C}$ attached to the divisor consisting of the identity on $\mathbb{C}/\Lambda$.

For reference, see ([1] Chapter 1) and ([25] Chapters 1, 4, 18).

1.1.1.2 Classical theta functions

Also in the 1850s, Riemann began the systematic study of similar higher-dimensional functions. Instead of taking an element τ in the upper half space, take τ to be a $g \times g$ symmetric matrix whose imaginary part is positive definite (the set of which is known as Siegel upper-half space), then define $\Lambda = \mathbb{Z}^g + \tau\mathbb{Z}^g$ and for z in $\mathbb{C}^g$ set

$$\vartheta(z) = \sum_{n \in \mathbb{Z}^g} e^{\pi i n^t \tau n + 2\pi i n^t z},$$

where ^{t} denotes the transpose. This function transforms nicely under Λ

$$\vartheta(z+m) = \vartheta(z)$$

$$\vartheta(z+\tau m) = e^{-\pi i m^t \tau m - 2\pi i m^t z}\vartheta(z)$$

for all m in $\mathbb{Z}^g$. The function $\vartheta(z)$ then must have a periodic vanishing locus Θ (if $g(z)$ is any holomorphic function on $\mathbb{C}^g$ then $e^{g(z)}$ is non-vanishing and entire). This analytic divisor thus descends to a divisor Θ on $\mathbb{C}^g/\Lambda$. Note that, like the Weierstrass σ function, the factor of automorphy under translation by Λ is the exponential of a linear form in z, hence the second logarithmic derivatives of $\theta(z)$ will be invariant under the action of Λ, so define rational functions on $\mathbb{C}^g/\Lambda$. See [43] Chapter 2 for a thorough discussion.

1.1.1.3 Kleinian sigma functions

In his 1886 and 1888 papers [23] and [24], Klein introduced a closely related function, denoted $\sigma(z)$ specifically for the τ arising from the periods of a hyperelliptic curve. As with $\vartheta(z)$, the second logarithmic derivatives of $\sigma(z)$ define rational functions on $\mathbb{C}^g/\Lambda$, but they have been described explicitly in terms of the underlying hyperelliptic curve. See H. F. Baker's 1898 paper [3] for the general theory, his 1907 book [4] for the genus two case, or Arledge and Grant [2] for a modern treatment.

1.1.1.4 General theta functions

Perhaps the most general definition of a theta function, found in some literature, is any holomorphic function on $\mathbb{C}^g$ which vanishes along Θ for some periodic divisor Θ. Different texts have different thresholds of properties which must be enjoyed by either Θ or the corresponding function to merit the moniker of theta function.

In more modern language, any theta function can be thought of as an explicit description of a section of a line bundle on the complex torus $\mathbb{C}^g/\Lambda$. If $\mathscr{L} \to \mathbb{C}^g/\Lambda$ is a line bundle, then pulling back along the universal covering map $\pi : \mathbb{C}^g \to \mathbb{C}^g/\Lambda$, the line bundle $\pi^*\mathscr{L}$ is trivial because all line bundles on $\mathbb{C}^g$ are trivial. Hence $\pi^*\mathscr{L} \cong \mathbb{C} \times \mathbb{C}^g$. After choosing such an isomorphism, for any section s of $\mathscr{L}$, π^*s becomes a function on $\mathbb{C}^g$. Oftentimes one restricts the type of line bundles one is looking at (perhaps to ample line bundles, for example) and the possible choices of trivializing isomorphism (the nicer the choice of isomorphism, the better the properties the associated theta functions can hope to have). See [46] and [8] for a discussion.

1.1.2 Algebraic theta functions

Several attempts have been made to devise algebraic theories which allow one to make use of the benefits of having theta functions for abelian varieties over more general fields, or even for other algebro-geometric objects which share structural properties with abelian varieties.

1.1.2.1 Mumford's finite theta functions

In 1966 [37][38][39], Mumford developed a theory of theta functions attached to an ample line bundle $\mathscr{L}$ on an abelian variety over an algebraically closed field. Unlike the classical functions which are entire functions on a universal cover of the associated abelian variety, Mumford's functions are defined on (often quite small) finite subgroups of A. Specifically, the line bundle $\mathscr{L}$ defines a map $\varphi_{\mathscr{L}} : A \to \hat{A}$ from A to its dual, and theta functions are defined on the kernel of this map. This map $\varphi_{\mathscr{L}}$ is the data of a polarization on A. The data of A along with a map $\varphi_{\mathscr{L}}$ is called a polarized abelian variety (said to be prinicipally polarized if the kernel of $\varphi_{\mathscr{L}}$ is trivial). We see that the closer to being principal the polarization is, the smaller the set of definition of the theta functions, which means for the line bundles often considered in the classical setting, these functions have very small domains.

On the other hand, the theta functions attached to $\mathscr{L}$ are compatible in a precise sense with those attached to $\mathscr{L}^n$, which have ever larger kernels. Taking limits, one gets theta functions defined on the Tate module of A.

1.1.2.2 Barsotti's theory

In his 1970 paper [6], Barsotti took as starting point the observation that

$$F_\vartheta(x, y, z) = \frac{\vartheta(x+y+z)\vartheta(x)\vartheta(y)\vartheta(z)}{\vartheta(x+y)\vartheta(x+z)\vartheta(y+z)}$$

is invariant under addition by Λ in each of x, y, z and thus defines an algebraic function on $(\mathbb{C}^g/\Lambda)^3$. This is an avatar of the theorem of the cube with respect to the associated line bundle, and under most common definitions of a theta function, this property holds (it is straightforward to check it for Riemann's function).

On an abelian variety A over a field of characteristic zero, Barsotti had a purely algebraic method to attach to any divisor D a power series ϑ_D such that F_{ϑ_D} was the expansion of a rational function on A^3. In particular if $p_i, p_{ij}, p_{123} : A^3 \to A$ are the morphisms defined by $p_i(x_1, x_2, x_3) = x_i$, $p_{ij}(x_1, x_2, x_3) = x_i + x_j$ and $p_{123}(x_1, x_2, x_3) = x_1 + x_2 + x_3$, then F_{ϑ_D} will have divisor $p_{123}^*D - p_{12}^*D - p_{13}^*D - p_{23}^*D + p_1^*D + p_2^*D + p_3^*D$.

Subsequent work of Cristante and Candilera [14][13] extended these ideas to positive characteristic which requires some thorough re-imagining and produces functions not in power series rings, but that exist in some perfection of power series rings. Barsotti [7] and Bottacin [11] also showed that it works just as well to consider functional expressions

$$G_\vartheta(x,y) = \frac{\vartheta(x+y)\vartheta(x-y)}{\vartheta(x)^2\vartheta(y)\vartheta(-y)}$$

which also descend to rational functions on $A \times A$ for classical theta functions. Many of these authors were interested not only in abelian varieties, but also other objects with similar behaviors (semi-abelian varieties, Barsotti–Tate groups, Tate modules).

1.1.2.3 Breen's cubical structures

In 1983 in [12], Breen succeeded in bringing together many of these ideas about theta functions and uniting them using the language of bi-extensions, due to Mumford in [41]. The use of bi-extensions also featured prominantly in the later papers of Cristante.

1.1.3 p-Adic theories

As early as the late 1950s, Tate began developing a parallel story to the complex picture for the p-adic context.

1.1.3.1 Tate curves

In Tate's original work on the subject, written in the 1950s but not published until the 1990s [53], he found that the function fields of some p-adic elliptic curves could be described as analytic functions periodic with respect to multiplication by an element q satisfying $|q| < 1$. These curves could be thought of as $\mathbb{Q}_p^*/\langle q\rangle$ in much the same way as a complex elliptic curve has a description as $\mathbb{C}^*/\langle e^{2\pi i\tau}\rangle$. In this setting, quasi-periodic functions with respect to multiplication by q take the place of quasi-periodic functions with respect to addition by λ.

Unfortunately, only elliptic curves with non-integral j-invariant can possibly admit this description. See Roquette's book [49] for details.

1.1.3.2 Morikawa

In 1961 [36], Morikawa brought Tate's idea to higher dimensional abelian varieties which admit descriptions as $\mathbb{Q}_p^g/\langle q_1, \ldots, q_g\rangle$. In his 1967 thesis [33], McCabe developed a similar theory. In 1972 [18], Gerritzen put these constructions on the formal footing of rigid geometry.

1.1.3.3 Cristante

In 1985 [15], for good ordinary reduction abelian varieties, to a totally symmetric divisor D avoiding the origin, Cristante used his earlier work to produce a p-adic theta function attached to D which has integral coefficients. When dropping the assumptions on D, he could also produce a theta function, but only after possibly extending the ground field.

1.1.3.4 Norman

Also in 1985 [47], Norman used limits of Mumford's finite theta functions to construct p-adic power series with integral coefficients for abelian varieties with ordinary reduction (and otherwise functions in perfections of power series rings). He also recast the work of Barsotti and Cristante in the same language as to make a direct comparison. His paper claims to require the assumption that the associated line bundles are totally symmetric, though I'm pretty sure his methods require only that the line bundle be symmetric.

In 1986 [48], Norman discussed writing his theta functions in terms of p-adic measures.

1.1.3.5 Mazur–Tate sigma function

In 1991 [29] (though appearing in applications first in 1983/1986 [28] [30]), for an ordinary (not necessarily good) reduction elliptic curve E given by $y^2 = x^3 + Ax + B$, Mazur and Tate produced a power series with integral coefficients, normalized by a choice of invariant differential ω on E, which mimics many basic properties of the complex σ function.

The Mazur–Tate paper developed a general theory of division polynomials which associates a meromorphic function Φ_f to any isogeny of elliptic curves $f : E_1 \to E_2$ over any field K. This

Φ_f is a meromorphic function on E_1 whose zeroes are the kernel of f and whose only pole is at the identity. The name stems from the case when f is the multiplication by m map $[m]_E : E \to E$, where $\Phi_{[m]_E}$ agrees with the classical m-th division polynomial on E.

When K is a field complete with respect to a non-archimedean absolute value with residue field k of positive residue characteristic $p > 2$ and E is an elliptic curve over F of ordinary reduction (either if E is of good reduction modulo a uniformizer π of K such that the reduced curve E_s satisfies $E_s(\overline{k}) \cong \mathbb{Z}/p\mathbb{Z}$ or if E is a Tate curve), Mazur and Tate considered the tower of étale p-power covers of E

$$\cdots \to E_3 \xrightarrow{a_{3,2}} E_2 \xrightarrow{a_{2,1}} E_1 \xrightarrow{a_1} E,$$

defining division polynomials ϕ_n to each of the isogenies $E_n \to E$. Using the $a_{n+1,n}$ to identify the formal groups at the origin on each curve, if t is a local parameter at the origin on E, its pullback is a local parameter at the origin on E_n and under this identification, functions $\sigma_n = t^{p^n}\phi_n$ can be defined. Considered in the adic topology, there is convergence $\sigma_n \to \sigma$. Aside from the precise method of construction being new relative to previous works, strong uniqueness properties of the σ function revolving around the integrality of the coefficients are shown to hold, which give something of a fundamentally different flavor to the theory than in the complex setting.

In a paper in preparation [9], the author and Grant reconstructed the Mazur–Tate σ function by focusing on the zeta function as the basic object and produce a sigma function via "anti-logarithmic differentiation." The zeta function in [9] is produced as a limit of functions ζ_n on an elliptic curve

$$E:\; y^2 = x^3 + a_1x^2 + a_2x + a_3$$

whose Hasse invariant H is invertible, such that $-\frac{d}{\omega}\zeta_n \equiv x + \beta_n \pmod{p^n}$, where ω is the invariant differential given by $\frac{dx}{2y}$ and β_n is a constant in $\mathbb{Z}[a_1, a_2, a_3][H^{-1}]$. Modulo p^n, β_n is the unique constant making the above differential equation have a solution in $\mathbb{Z}[a_1, a_2, a_3][H^{-1}][[t]][t^{-1}]$. This gives rise to a unique β in the p-adic completion of $\mathbb{Z}[a_1, a_2, a_3][H^{-1}]$ such that $\frac{d}{\omega}\zeta_n \equiv x + \beta$ has a solution. The unique odd solution to this equation is the zeta function. Furthermore, as is shown by Mazur and Tate, this β has a life as a p-adic modular form, a multiple of the Eisenstein series of weight two.

1.2 This thesis

This thesis is broken into three parts. The first part, found in Chapter 2, generalizes the paper of Mazur and Tate [29] from elliptic curves to principally polarized abelian varieties of any dimension given a specific choice of symmetric theta divisor for the polarization.

Let K be a field complete with respect to a non-archimedean absolute value with ring of integers R and residue field k of characteristic $p \geq 3$ and let A be an abelian variety over K with good ordinary reduction. Fix a choice of symmetric theta divisor Θ on A, along with a choice of rational function g representing Θ near 0. The ordinary assumption provides a tower of étale isogenies

$$\cdots \to A_3 \xrightarrow{a_{3,2}} A_2 \xrightarrow{a_{2,1}} A_1 \xrightarrow{a_1} A$$

each of degree p^g. On each A_n the choice of Θ induces a unique choice of symmetric theta divisor Θ_n. Fix a choice of functions g_n representing Θ_n near 0_n. If $a_n = a_{n,n-1} \circ \cdots a_{2,1} \circ a_1$, there are division polynomials ϕ_n on A_n defined by the property that their associated divisor $(\phi_n) = a_n^* \Theta - p^n \Theta_n$ and normalized by the choice of the g_n. If $T_1, \ldots, T_g$ are local parameters to 0 on A, then $a_n^* T_1, \ldots, a_n^* T_g$ are local parameters to 0_n on A_n. Identifying $a_n^* T_i$ with T_i, the functions $\sigma_n = g_n^{p^n} \phi_n$ converge to a power series $\sigma = \sigma_{\Theta,g}$ in $R[[T_1, \ldots, T_g]]$. This limit is independent of the choices of the functions g_n used to define it.

In Section 2.3, this series σ is shown to have many of the properties one might expect of theta functions. For example, σ is an even or odd function depending on whether Θ is even or odd. Similarly, if D_1 and D_2 are invariant derivations on A, then $D_2 D_1 \log(\sigma) = D_2 \frac{D_1 \sigma}{\sigma}$ is the power series expansion of a rational function on A with a pole of order two along Θ.

Note that the theta functions of Norman and Cristante are also power series in $T_1, \ldots, T_g$ with coefficients in R but for different divisors X on A. Both Norman and Cristante assume that

X is totally symmetric (i.e., there exists some other divisor X' such that $X = X' + [-1]^*X'$); while Norman's limit of Mumford algebraic theta functions requires X to be ample, Cristante's approach generalizing Barsotti's algebraic theta functions to positive characteristic and then lifting back to characteristic zero works for any totally symmetric X. The present approach works instead for specifically those divisors Θ which induce principal polarizations while only requiring symmetry of Θ (totally symmetric divisors are never principal). If $X = \Theta + \Theta$ then the square of the theta function θ_Θ^2 produced in this thesis for Θ agrees with the theta functions θ_X of Norman and Cristante for X. Thus θ_Θ can essentially be computed by $\sqrt{\theta_X}$ (the theta functions of Norman and Cristante are defined only up to scalar multiple whereas θ_Θ is defined precisely by the choices made). The corresponding properties to those in Section 2.3 (with the exception of evenness) are not explicitly worked out in the papers of Norman or Cristante, though a "cubical" version of Proposition 17 appears in both.

The second part of the thesis, located in Chapter 3, generalizes work in [9] on p-adic Weierstrass zeta functions on elliptic curves to curves of genus two with specified Weierstrass point. Let C be the genus two curve given by affine model

$$y^2 = x^5 + b_1x^4 + b_2x^3 + b_3x^2 + b_4x + b_5$$

defined over the ring $\mathbb{Q}(b_1, \ldots, b_5)$. The role of the Hasse invariant is replaced by the determinant H of the Hasse–Witt matrix. Here, a sequence of pairs of differential equations modulo p^n are considered

$$-\frac{d}{\omega}\zeta_{1,n} = 3x^3 + 3b_1x^2 - \alpha_n x - (3b_1b_2 - b_1\alpha_n + 3b_3 + 3\delta_n) \pmod{p^n}$$
$$-\frac{d}{\omega}\zeta_{2,n} = x^2 - \beta_n x - (b_2 - b_1\beta_n + 3\gamma_n) \pmod{p^n}$$

where ω is the differential given by $\frac{dx}{2y}$. Solutions to these are found in $\mathbb{Z}[b_1, \ldots, b_5][H^{-1}][[t]][t^{-1}]/p^n$ for the local parameter to the point at infinity $t = -\frac{x^2}{y}$. These functions admit well-defined limits $\zeta_{1,n} \to \zeta_{C,1}$ and $\zeta_{2,n} \to \zeta_{C,2}$ as Laurent series with coefficients in the p-adic completion of $\mathbb{Z}[b_1, \ldots, b_5][H^{-1}]$. The Laurent series $\zeta_{C,1}$ and $\zeta_{C,2}$ are the unique odd solutions to differential equations

$$-\frac{d}{\omega}\zeta_1 = 3x^3 + 3b_1x^2 - \alpha x - (3b_1b_2 - b_1\alpha + 3b_3 + 3\delta)$$

$$-\frac{d}{\omega}\zeta_2 = x^2 - \beta x - (b_2 - b_1\beta + 3\gamma)$$

with the four constants α, β, δ, and γ (themselves limits of the α_n, β_n, δ_n and γ_n respectively) playing the role of the p-adic Eisenstein series of weight 2.

These $\zeta_{C,1}$ and $\zeta_{C,2}$ are then universal in the sense that for a smooth genus two curve $\tilde{C}$ with coefficients in a p-adically complete ring R with an affine equation

$$y^2 = x^5 + a_1x^4 + a_2x^3 + a_3x^2 + a_4x + a_5$$

and invertible Hasse–Witt matrix, under the specialization map sending $b_i \mapsto a_i$, the series $\zeta_{C,1}$ and $\zeta_{C,2}$ pull back to give $\zeta_{\tilde{C},1}$ and $\zeta_{\tilde{C},2}$ which are Laurent series with coefficients in R.

The final part of the thesis, Chapter 4, details of the sigma function from the first part are worked out explicitly for Jacobians of curves of genus two. Let K be a local field of characteristic 0 with ring of integers R, uniformizer π and residue field k of characteristic $p > 2$. For a curve C defined by affine model

$$y^2 = x^5 + b_1x^4 + b_2x^3 + b_3x^2 + b_4x + b_5$$

with coefficients in R, no repeated roots modulo π, and invertible Hasse–Witt matrix, the Jacobian of C will be an abelian surface over K of good ordinary reduction. The Weierstrass point ∞ at infinity on C gives a distinguished embedding of C into its Jacobian $J = \mathrm{Jac}(C)$. The image of this embedding, Θ, is a symmetric (odd) theta divisor in the principally polarized abelian variety J so together $\mathrm{Jac}(C)$ and Θ give the required inputs of Chapter 2 to have a σ function in the previous sense.

Looking more closely, the Abel–Jacobi map with ∞ as basepoint gives an explicit birational map $\Phi : C^{(2)} \to J$ under which the image of the set of points of the form $P + \infty$ yields the above embedding $C \to J$. This enables one to explicitly describe the function theory on J in terms of the functions on C.

For example, if $\overline{d} = \frac{d}{\omega}$ where ω is the differential given by $\frac{dx}{2y}$, then

$$D_1 = \frac{x_1\overline{d}_2 - x_2\overline{d}_1}{x_1 - x_2}$$

$$D_2 = \frac{\overline{d}_1 - \overline{d}_2}{x_1 - x_2}$$

are derivations on the function field of C^2 (where x_i is interpreted as the x function on the i-th factor of $C \times C$, etc.) which are invariant under the action of the symmetric group on the indices and thus define derivations on the symmetric square $C^{(2)}$. Then these are also derivations on the function field of J, and are in fact a basis of the invariant differentials on J. The role played by the x function on an elliptic curve is replaced by three functions $\wp_{11}$, $\wp_{12}$, $\wp_{22}$ given by formulas

$$\wp_{11} = \frac{(x_1+x_2)(x_1x_2)^2 + 2b_1(x_1x_2)^2 + b_2(x_1+x_2)(x_1x_2) + 2b_3(x_1x_2) + b_4(x_1+x_2) + 2b_5 - 2y_1y_2}{x_1 - x_2}$$

$$\wp_{12} = -x_1x_2$$

$$\wp_{22} = x_1 + x_2$$

and the role of $2y$ is played by four functions $\wp_{111}$, $\wp_{112}$, $\wp_{122}$, $\wp_{222}$ (they have similarily explicit formulas which can be found in Chapter 4). Then similiarly to the situation for elliptic curves, there are identities

$$D_jD_i\log(\sigma) = -\wp_{ij} + c_{ij}$$

$$D_\ell D_jD_i\log(\sigma) = -\wp_{ij\ell}$$

for some constants c_{ij}.

There are now two different ways to construct zeta-like series on J. The first is to take logarithmic derivatives of σ, yielding

$$\zeta_{J,1} = D_1\log(\sigma) = \frac{D_1\sigma}{\sigma}$$

$$\zeta_{J,2} = D_2\log(\sigma) = \frac{D_2\sigma}{\sigma}.$$

The second is to take the sum of two copies of the zeta functions on C from Chapter 3, which gives

$$\xi_1 = (\zeta_{C,1})_1 + (\zeta_{C,1})_2$$

$$\xi_2 = (\zeta_{C,2})_1 + (\zeta_{C,2})_2.$$

We prove that these two different constructions are related by

$$\zeta_{J,1} = \xi_1 - b_1\xi_2 + \frac{1}{2}\wp_{222}$$

$$\zeta_{J,2} = \xi_2$$

as Laurent series in $t_1 + t_2$ and t_1t_2, where $t = -\frac{x^2}{y}$ is a local parameter to ∞ on C.

1.2.0.1 Prerequisites

Each chapter begins with the necessary prerequisites. Chapters 2 and 3 are logically independent of one another, while Chapter 4 assumes everything that comes before.

Chapter 2

Sigma functions on abelian varieties

2.1 Preliminaries on abelian varieties

2.1.1 Abelian varieties

An (algebraic) variety will be taken to mean a separated geometrically integral scheme of finite type over a field. It is entirely determined by its collection of closed points and will often be conflated with its restriction to this set. A variety will be said to be projective if it is given as the vanishing locus of homogenous polynomials inside projective space.

A group variety G over a field F is a variety over F whose closed points form a group, where the operation and inversion are given by morphisms of varieties. Group varieties can be understood in the greater context of group schemes (which are discussed in section 2.1.5). An abelian variety A over a field F is a projective group variety over F (which necessarily must be commutative). References include [46], [17], [34].

2.1.2 Line bundles

The collection of line bundles on A form a group. If one restricts attention to those line bundles algebraically equivalent to the trivial line bundle, this group parameterizes points on another abelian variety A^t defined over F. For any point P on A, since A is a group variety, there is a translation morphism $T_P : A \to A$ taking $x \mapsto P + x$. This induces a map on line bundles $\mathscr{L} \mapsto T_P^* \mathscr{L}$. If $\mathscr{L}$ is a line bundle on A, then the theorem of the square implies there is a homomorphism of group varieties $\varphi_{\mathscr{L}} : A \to A^t$ defined by $x \mapsto T_x^*\mathscr{L} \otimes \mathscr{L}^{-1}$. We say $\mathscr{L}$ is nondegenerate if this homomorphism is an isogeny (surjective with finite kernel). In particular, if $\mathscr{L}$ is ample, it is nondegenerate. Any such isogeny, for $\mathscr{L}$ ample, is said to be a polarization on A. Note that the polarization isogeny may be defined over a field smaller than that of $\mathscr{L}$.

Throughout this section, the notation $p \in A$ is meant to mean a functorial point of A (i.e., an element of $A(S)$ for some F-scheme S (see [46] page 228).

Proposition 1. *Let $A \xrightarrow{f} B$ be an isogeny of abelian varieties, all defined over F, and let M be a line bundle on B, L a line bundle on A such that $L \cong f^*M$. Then the diagram*

$$\begin{tikzcd}
A \arrow[r, "\varphi_L"] \arrow[d, "f"'] & \hat{A} \\
B \arrow[r, "\varphi_M"] & \hat{B} \arrow[u, "f^*"']
\end{tikzcd}$$

commutes.

Proof. Let $p \in A$. Then

$$\begin{aligned}
f^*(\varphi_M(f(p))) &\cong f^*(T^*_{f(p)}M \otimes M^{-1}) && \text{definition of } \varphi_M \\
&\cong f^*(T^*_{f(p)}M) \otimes f^*(M)^{-1} && f^* \text{ is a homomorphism} \\
&\cong T_p^* f^*M \otimes (f^*M)^{-1} && f \circ T_p = T_{f(p)} \circ f \\
&\cong \varphi_{f^*M}(p) && \text{definition of } \phi_L \\
&\cong \varphi_L(p) && L \cong f^*M.
\end{aligned}$$

□

Remark: cf. the beginning of the proof of Theorem 1 in [46].

We are interested in $\ker \varphi_L$. Here kernels are taken in the category of group schemes, so are group schemes themselves. If φ_L is separable, then $\ker \varphi_L$ will be reduced (i.e., it will be determined by its collection of closed points of A).

Corollary 2. *With notation as in the proposition,*

$$\varphi_M^{-1}(\ker(f^*)) = f(\ker \varphi_L)$$

as group schemes.

Proof. Since $\varphi_L = f^* \circ \varphi_M \circ f$ from above, we have

$$\begin{aligned}\ker(\varphi_L) &= \ker(f^* \circ \varphi_M \circ f)\\ f(\ker(\varphi_L)) &= f(\ker(f^* \circ \varphi_M \circ f))\\ &= f\left((f^* \circ \varphi_M \circ f)^{-1}(0)\right)\\ &= f\left(f^{-1} \circ \varphi_M^{-1} \circ {f^*}^{-1}(0)\right)\\ &= \varphi_M^{-1} \circ {f^*}^{-1}(0).\end{aligned}$$

We get $f(K(L)) = \varphi_M^{-1}(\ker(f^*))$. □

Corollary 3. *Let $A \xrightarrow{f} B$ be an isogeny of abelian varieties, M be a nondegenerate line bundle on B, and L a nondegenerate line bundle on A such that $L \cong f^*M$. Suppose also that $\varphi_M : B(F) \to \hat{B}(F)$ is surjective (always true when the degree of φ_M is relatively prime to the characteristic of F and F is algebraically closed). Then a line bundle M' on B satisfies $f^*M \cong f^*M'$ if and only if $M' \cong T_p^*M$ for some $p \in f(\ker \varphi_L)$.*

Proof. If $f^*M' \cong f^*M$, we get $f^*(M' \otimes M^{-1}) = 1$ and hence $M' \otimes M^{-1} \in \ker(f^*)$. By the previous corollary and the surjectivity of φ_M, this happens if and only if there exists $p \in f(\ker \varphi_L)$ such that $M' \otimes M^{-1} \cong \varphi_M(p)$. This holds if and only if

$$\begin{aligned}M' &\cong \varphi_M(p) \otimes M\\ &\cong T_p^*M \otimes M^{-1} \otimes M\\ &\cong T_p^*M.\end{aligned}$$

□

2.1.2.1 Divisors attached to principally polarizing line bundles

In general, a section s of a line bundle $\mathscr{L}$ over a variety X defines a divisor (s) on X by recording the zeroes and poles of s. All the sections of $\mathscr{L}$ differ by multiplication of a meromorphic function, hence the linear equivalence class of (s) is uniquely determined by $\mathscr{L}$ (the converse is also true, so we denote $\mathcal{L}(D)$ to be the line bundle determined by the linear equivalence class of the divisor D).

If $\mathscr{L}$ is an ample principally polarizing line bundle on an abelian variety A over a field F, then $\dim H^0(A, \mathscr{L}) = 1$, hence there is a unique effective divisor Θ in the linear equivalence class determined by $\mathscr{L}$. In the case that $\mathscr{L}$ is symmetric, i.e., $[-1]^*\mathscr{L} \cong \mathscr{L}$, we have

$$\mathcal{L}([-1]^*\Theta) \cong [-1]^*\mathscr{L} \cong \mathscr{L} \cong \mathcal{L}(\Theta)$$

so therefore $[-1]^*\Theta \sim \Theta$, where $\sim$ denotes linear equivalence. Since Θ is the unique effective divisor defining $\mathscr{L}$, we get $[-1]^*\Theta = \Theta$.

2.1.2.2 Symmetric divisors

We wish to develop a notion of "even" versus "odd" for symmetric divisors on an abelian variety A over F. A divisor D is said to be symmetric if $[-1]^*D = D$. We will say a function g on A **locally represents** a divisor D on a neighborhood U if $D|_U$ is $(g|_U)$ on U. If D is locally represented by g on some neighborhood of the identity U, then after restricting to $U \cap [-1]U$, we have $[-1]^*g = g \cdot u$ for some meromorphic function u which neither vanishes nor has a pole on $U \cap [-1]U$. Since $g = [-1]^*[-1]^*g = [-1]^*(g \cdot u) = g \cdot u \cdot [-1]^*u$, we must have $1 = u \cdot [-1]^*u$. We can look at the formal expansion at the origin of u, as a power series in $K[[t_1, \dots, t_g]]$ for a choice of local parameters at the origin $t_1, \dots, t_g$. In particular, we can choose the t_i to be odd if the characteristic of F is not 2 by taking $t_i = \frac{t'_i - [-1]^*t'_i}{2}$ for any set of local parameters at the origin $t'_1, \dots, t'_g$. This gives an expression $u = a_0 + \sum_I a_I t^I$ where the I run over indices in $\mathbb{N}^g$, not all entries zero and $t^I = t_1^{i_1} \cdots t_g^{i_g}$ if $I = (i_1, \dots, i_g)$. Then $[-1]^*u = a_0 + \sum (-1)^{|I|} a_I t^I$. Multiplying out, we have

$$1 = u \cdot [-1]^*u = \left(a_0 + \sum_I a_I t^I\right) \cdot \left(a_0 + \sum_I \pm a_I t^I\right) = a_0^2 + O(\text{degree } 2)$$

and hence

$$a_0 = \pm 1.$$

This is independent of the choice of $t_1, \ldots, t_g$, but more is true.

Lemma 4. *This a_0 is independent of the representative g used to represent D near the origin.*

Proof. Let g' represent D on some neighborhood U' of the origin such that $[-1]^*g' = g' \cdot u'$ on $U' \cap [-1]U'$ with $u' = a_0' + \sum_I a_I' t^I$ and let $V = U \cap [-1]U \cap U' \cap [-1]U'$. Then there is some meromorphic function ℓ which neither vanishes nor has a pole on V such that $g' = g \cdot \ell$. There is an expansion $\ell = b_0 + \sum_I b_I t^I$. Since ℓ does not vanish at the origin, $b_0 \neq 0$ so after possibly scaling g' by $\frac{1}{b_0}$, we can take $b_0 = 1$ (scaling g' does not affect u'). Acting by $[-1]^*$, we have $g' \cdot u' = g \cdot u \cdot [-1]^*\ell$. Combining, we have $\ell = \frac{g'}{g} = \frac{u}{u'}[-1]^*\ell$, or that

$$u' \cdot \ell = u \cdot [-1]^*\ell.$$

Since $[-1]^*\ell = 1 + \sum_I \pm b_I t^I$, we see looking at the constant terms in the above expression, that we have $a_0' \cdot 1 = a_0 \cdot 1$. □

We will define a symmetric D to be **even** or **odd** by whether the associated a_0 is 1 or -1, respectively.

2.1.3 Models

Fix a rational prime p. A local field K is a field which is a finite extension of $\mathbb{Q}_p$ or $\mathbb{F}_p((t))$. One may start with an abelian variety A over a local field K and wish to extend the variety to be a scheme over R, the ring of integers of K. In general, a scheme over R which after base change to K is isomorphic to A, is said to be an R-model for A. Throughout the thesis we shall denote the special fiber of a scheme X over R by X_s.

2.1.3.1 Projective models

For example, since A is projective, it is given as a closed subscheme of some projective space $\mathbb{P}^r_K$ defined by some homogenous ideal $\mathfrak{a}$ of $K[x_0, \ldots, x_r]$. For each polynomial in $\mathfrak{a}$, after multiplying or dividing by an appropriate multiple of a uniformizer π of R, each of these polynomials is defined over R while not being divisible by π. The collection of resulting normalized polynomials is precisely $\mathfrak{a} \cap R[x_0, \ldots, x_r]$, which we will call $\mathfrak{a}_R$. The resulting homogenous ideal is now defined over R and defines a projective scheme $A_{\mathfrak{a}}$ which is a closed subspace of $\mathbb{P}^r_R$ and is an R-model for A. This model depends on the choice of ideal $\mathfrak{a}$ (i.e., the embedding of A into projective space); if a different set of defining equations over K is used, the R-structure of the model may be different.

2.1.3.2 Néron models

While there are always projective models for an abelian variety over K, the special fiber $A_{\mathfrak{a},s}$ (taking all of the elements of $\mathfrak{a}_R$ modulo π and considering the resulting algebraic set over the residue field k) may not be well behaved. In particular, it may not be smooth, which precludes it from being itself an abelian variety. Instead, one often wishes to have a model which is a group scheme over R. The theory of Néron models produces exactly such a group scheme.

For an abelian variety A over a given local field K, the Néron model $\mathcal{A}$ is a group scheme which is an R-model for A and satisfies the Néron mapping property: if $\mathcal{X}$ is a smooth separated R scheme with a morphism of K-schemes $\mathcal{X}_K \to A$, then the morphism extends uniquely to an R morphism $\mathcal{X} \to \mathcal{A}$. An account of the theory is discussed in detail in [10]. In particular, the Néron model always exists. It is preserved under base change by unramified extensions of R but not in general by ramified extensions.

2.1.3.3 Abelian schemes

In the case where there is a nonsingular projective model for A (i.e., there is a choice of defining ideal $\mathfrak{a}$ such that $A_{\mathfrak{a}}$ is smooth over R), the group law on A extends to $A_{\mathfrak{a}}$, is defined over R and this projective model is the Néron model $\mathcal{A}$ of A. This is equivalent to the Néron model being projective and implies that the Néron model is stable under arbitrary extensions of R. In this situation, A is said to have good reduction and $\mathcal{A}$ is called an abelian scheme. The standard reference is [40], Chapter 6.

2.1.4 Ordinary reduction

An abelian variety defined over a field k of positive characteristic p has a wider range of possible structures on its p-torsion than in the prime-to-characteristic case. In the prime-to-characteristic case, over an algebraically closed field, the only possibility is that $A[p] \cong (\mathbb{Z}/p\mathbb{Z})^{2g}$, a reduced finite flat group scheme with p^{2g} points. Over an algebraically closed field of characteristic p, we have $A[p] \cong (\mathbb{Z}/p\mathbb{Z})^s \times \mu_p^s \times M$ where M is some connected group scheme of order $p^{2(g-s)}$ isomorphic to its own Cartier dual (see [46], page 147). In fact, the same decomposition is true of the p^n-torsion: $A[p^n] \cong (\mathbb{Z}/p^n\mathbb{Z})^s \times \mu_{p^n}^s \times M_n$ for a fixed s. Over an algebraically closed field, A is said to be ordinary if $s = g$, which is the same as $M = 0$. Over an arbitrary field of characteristic p, A is said to be ordinary if it is ordinary over an algebraic closure.

Over a local field K, an abelian variety A is said to be of ordinary reduction if, for the Néron model $\mathcal{A}$ of A, we have $\mathcal{A}[p] \cong (\mathbb{Z}/p\mathbb{Z})^g \times \mu_p^g$, over some unramified extension of the ring of integers R. The connected component containing the identity of $\mathcal{A}[p]$ is defined over R and is called the canonical subgroup (it is the p-torsion in the formal group at the origin). By the above, it is isomorphic to μ_p^g after an unramified extension of R.

2.1.5 Group schemes

See ([54] Sections 1 and 2), ([10] Section 4.1), or ([46] Section 11) for reference. A group scheme G over the ring R is a group object in the category of schemes over R. That is to say that there are morphisms $m : G \times G \to G$, $\iota : G \to G$, and $\epsilon : \mathrm{Spec}(R) \to G$ satsifying certain compatabilities demanded by the commuting of various diagrams.

Associativity:

$$\begin{tikzcd}
G \times G \times G \arrow[r, "m\times \mathrm{id}"] \arrow[d, "\mathrm{id}\times m"'] & G \times G \arrow[d, "m"] \\
G \times G \arrow[r, "m"] & G
\end{tikzcd}$$

Inverses:

$$\begin{tikzcd}
G \arrow[r, "\iota\times\mathrm{id}"] \arrow[dr, "\mathrm{id}"'] & G \times G \arrow[d, "m"] \\
& G
\end{tikzcd}
\qquad
\begin{tikzcd}
G \arrow[r, "\mathrm{id}\times\iota"] \arrow[dr, "\mathrm{id}"'] & G \times G \arrow[d, "m"] \\
& G
\end{tikzcd}$$

Identity:

$$\begin{tikzcd}
G \times \mathrm{Spec}(R) \arrow[r, "\mathrm{id}\times\epsilon"] \arrow[dr, "p_1"'] & G \times G \arrow[d, "m"] \\
& G
\end{tikzcd}
\qquad
\begin{tikzcd}
\mathrm{Spec}(R) \times G \arrow[r, "\epsilon\times\mathrm{id}"] \arrow[dr, "p_2"'] & G \times G \arrow[d, "m"] \\
& G
\end{tikzcd}$$

The commuting of these diagrams is equivalent to the functorial points of G being groups, i.e., that $\mathrm{Hom}_R(S, G)$, the set of morphisms of R-schemes, naturally carries the structure of a group for every R-scheme S. If, in addition, the following diagram commutes, G is said to be commutative:

$$\begin{tikzcd}
G \times G \arrow[r, "\tau"] \arrow[dr, "m"'] & G \times G \arrow[d, "m"] \\
& G
\end{tikzcd}$$

where τ is the map which swaps factors. All group schemes appearing in this thesis will be commutative, so we will rename $\iota = [-1]$ and $\epsilon = 0_G$. We will also identify 0_G with its image in G.

A homomorphism of commutative group schemes over R, $f : G \to H$ is a morphism of R-schemes which commutes with the morphisms m, $[-1]$, and 0 in the sense that the following diagrams commute:

$$\begin{tikzcd}
G \times G \arrow[r, "m_G"] \arrow[d, "f\times f"'] & G \arrow[d, "f"] \\
H \times H \arrow[r, "m_H"] & H
\end{tikzcd}
\qquad
\begin{tikzcd}
G \arrow[r, "{[-1]_G}"] \arrow[d, "f"'] & G \arrow[d, "f"] \\
H \arrow[r, "{[-1]_H}"] & H
\end{tikzcd}
\qquad
\begin{tikzcd}
\mathrm{Spec}(R) \arrow[r, "0_G"] \arrow[dr, "0_H"'] & G \arrow[d, "f\ ."] \\
& H
\end{tikzcd}$$

One example of a homomorphism of commutative group schemes is the multiplication by n endomorphism. Let n be a positive integer, then let $[n] : G \to G$ be the morphism produced by adding an element to itself n times (in the language of diagrams, this can be achieved by composing the diagnal map $G \to G^n$ followed by a succession of m maps). Commutivity of G forces $[n]$ to be an endomorphism of group schemes.

2.1.6 Formal groups

For reference, see ([50] Section 5) and ([26] Section 10.1.3 and Exercises 10.1.15-16). Let K be a local field with ring of integers R with uniformizer π and residue field k, and let $\mathcal{G}$ be a commutative (reduced) group scheme of dimension d defined over R, with generic fiber G which will necessarily be an algebraic group over K. Since $\mathcal{G} \to \operatorname{Spec} R$ is smooth, then for any section r, the completion $\hat{\mathcal{O}}_{\mathcal{G},r} \cong R[[t_1, \ldots, t_d]]$ for any collection $t_1, \ldots, t_d$ of local parameters at s defined over R. This is Exercise 6.2.1 in [26]. Let P in $\mathcal{G}(R)$ be given by r, then for any point P' in $\mathcal{G}(R)$ which reduces to the reduction of P on $\mathcal{G}_s$, $|t_i(P')|_\pi < 1$, hence any power series in the t_i with coefficients in R will converge when evaluated at P'. We will be particularly interested in the case when $P = 0_{\mathcal{G}}$.

The morphisms m, $[-1]$, and $0_{\mathcal{G}}$ induce maps on the structure sheaves $m^*\mathcal{O}_{\mathcal{G}} \to \mathcal{O}_{\mathcal{G}} \otimes \mathcal{O}_{\mathcal{G}}$, $[-1]^* : \mathcal{O}_{\mathcal{G}} \to \mathcal{O}_{\mathcal{G}}$ and $0_{\mathcal{G}}^* : \mathcal{O}_{\mathcal{G}} \to R$ which satisfy the same compatabilities as m, $[-1]$, and $0_{\mathcal{G}}$ with the arrows reversed. Because $m(0_{\mathcal{G}}, 0_{\mathcal{G}}) = 0_{\mathcal{G}}$ and $[-1](0_{\mathcal{G}}) = 0_{\mathcal{G}}$, the maps m^*, $[-1]^*$, and $0_{\mathcal{G}}^*$ extend to the stalk $\mathcal{O}_{\mathcal{G},0_{\mathcal{G}}}$ and thus to its completion $\hat{\mathcal{O}}_{\mathcal{G},0_{\mathcal{G}}}$.

Following this through with a choice of local parameters $t_1, \ldots, t_d$, we see the map $m^* : R[[t_1, \ldots, t_d]] \to R[[t_1, \ldots, t_d, t'_1, \ldots, t'_d]]$ is given by d power series $m_i(t_1, \ldots, t_d, t'_1, \ldots, t'_d)$ without constant terms, the map $[-1]^* : R[[t_1, \ldots, t_d]] \to R[[t_1, \ldots, t_d]]$ is given by d power series $\iota_i(t_1, \ldots, t_d)$ without constant terms, and the map $0_{\mathcal{G}}^* : R[[t_1, \ldots, t_d]] \to R$ sends each of the t_i to zero. The relations between these maps imply that for X, Y, and Z d-tuples of variables,

$$m^*(X, Y) = m^*(Y, X)$$

$$m^*(X, m^*(Y, Z)) = m^*(m^*(X, Y), Z)$$

$$m^*(X, [-1]^*X) = 0$$

$$m^*(X, 0) = X.$$

This is exactly the data of a d-dimensional commutative formal group law over R (see [22] for a reference).

The ring $\hat{\mathcal{O}}_{\mathcal{G},0_{\mathcal{G}}}$ can be interpreted as functions on all R-points of $\mathcal{G}$ reducing to the identity on the special fiber $\mathcal{G}_s$. We will denote this set $\mathcal{G}^f(R)$ and call it the R-points of the formal group $\mathcal{G}^f$. The choice of isomorphism $\hat{\mathcal{O}}_{\mathcal{G},0_{\mathcal{G}}} \cong R[[t_1,\ldots,t_d]]$ gives the points $\mathcal{G}^f(R)$ a bijection with the points $(\pi R)^d$, natural in R (see [26] Exercise 101.16). If we do not refer to R, by the points of $\mathcal{G}^f$ we mean the union of all $\mathcal{G}^f(S)$ where S is the ring of integers of an algebraic extension of K.

If P is an R-point of $\mathcal{G}^f$, the translation-by-P morphism T_P is the composition of maps $(\mathrm{id}, P) : \mathcal{G} \to \mathcal{G} \times \mathcal{G}$ sending $x \mapsto (x, P)$ and m. Following this through with the choice of local parameters $t_1,\ldots,t_d$, we see $(\mathrm{id}, P)^* : R[[t_1,\ldots,t_d,t'_1,\ldots,t'_d]] \to R[[t_1,\ldots,t_d]]$ is defined by $t_i \mapsto t_i$, $t'_i \mapsto t_i(P)$, where the $t_i(P)$ have absolute value less than one because P reduces to the origin on the special fiber. Composing gives the map $T_P^* = (\mathrm{id}, P)^* \circ m^* : R[[t_1,\ldots,t_d]] \to R[[t_1,\ldots,t_d]]$ defined by $t_i \mapsto m_i(t_1,\ldots,t_g,t_1(P),\ldots,t_g(P))$. The coefficients of T_P^* will be in R since the m_i have coefficients in R and each $t_i(P)$ has absolute value less than one. In particular, if f is in $R[[t_1,\ldots,t_d]]$, then $T_P^* f$ is also in $R[[t_1,\ldots,t_d]]$.

2.2 p-Adic sigma functions on abelian varieties

The goal of the present chapter is to generalize the construction of the p-adic σ function attached to an elliptic curve as in [29] to general principally polarized abelian varieties defined over a local field.

Throughout the chapter, let K be a local field with ring of integers R, uniformizer π and residue field k of characteristic p. Denote its absolute value by $|\cdot|_\pi$. We will consider a principally polarized abelian variety A with polarization $\varphi_{\mathscr{L}}$ all defined over K. The prime p will need to be odd for much of what follows.

We have already seen that an ample line bundle $\mathscr{L}$ inducing the polarization $\varphi_{\mathscr{L}}$ is determined uniquely by an effective divisor Θ. On the other hand, the isogeny $\varphi_{\mathscr{L}}$ determines $\mathscr{L}$ (and hence Θ) only up to translation (this defines Θ up to algebraic equivalence).

Note that in dimension one, an elliptic curve has not only a principal polarization, but a canonical choice of divisor given by the origin. Because we want to construct actual functions, along with a principally polarized abelian variety A of dimension g defined over K, we also want to consider a choice of a specific effective divisor $\Theta \subseteq A$ defined over K satisfying

(1) Θ is symmetric, i.e., $[-1]^*\Theta = \Theta$

(2) $\mathcal{L}(\Theta)$ is a line bundle inducing the principal polarization φ_L on A.

A divisor Θ of A satisfying the above conditions is said to be a symmetric theta divisor of A (a divisor satisfying only (2) is said to be a theta divisor of A). Any two theta divisors are translates of one another and the symmetric theta divisors differ by points of $A[2]$. Note that in general for an arbitrary principal polarization on A, a corresponding Θ may only be defined over an extension field of K, hence assuming we have such a choice to make is a nontrivial assumption.

For example, if A is the Jacobian J of a genus two curve C, such a choice of an odd symmetric theta divisor is provided by a choice of Weierstrass point on the curve and then Θ is the image of C under the Abel-Jacobi embedding of C into J using this point as basepoint. Over $\overline{K}$, there are six such choices (and 10 other translates which are also symmetric but are even and do not contain the identity), but it is possible that no such choice is K-rational.

Following Mazur and Tate, to construct a σ function associated to our choice of a symmetric theta divisor Θ, we will take a limit involving division polynomials associated to certain "nice" isogenies covering A, which will converge uniformly on the kernel of reduction of A. First we develop the theory of division polynomials attached to the nice class of isogenies of abelian varieties over an arbitrary field (which in dimension one includes all isogenies). We ultimately construct σ functions for abelian varieties of good ordinary reduction with a choice of a symmetric theta divisor Θ defined over K with the added data of a local representative for Θ (defined over R) in a neighborhood of the origin.

2.2.1 Division polynomials

Here we work to generalize the objects of ([29] Appendix I) to higher dimensions. For reference on technical details, see ([46] Section 23, especially page 231). Let A be an abelian variety defined over a field F. If A has a principally polarizing line bundle $\mathscr{L}$ over F, then $\mathscr{L}^n$ induces a Galois-equivariant nondegenerate antisymmetric bilinear pairing

$$A[n] \times A[n] \to \mu_n$$

called the Weil pairing attached to $\mathscr{L}^n$. If H is an F-rational subgroup of $A[n]$ which is a maximal isotropic subgroup under this pairing (meaning that its base change to $\overline{F}$ is maximal isotropic with respect to the pairing) and $u : A \to A'$ is an isogeny with kernel H, then there exists a principally polarizing line bundle $\mathscr{L}'$ on A' such that $u^*\mathscr{L}' \cong \mathscr{L}^n$. If H is defined over F, then because the isogeny $u : A \to A'$ is the quotient of A by a finite flat group scheme over F, A' and u must also be defined over F (see [54] p.135, [17] 4.39 and 4.40, or [46] Section 12). Furthermore, by Corollary 3 all such $\mathscr{L}'$ differ by translation by an element of $u(A[n])$. For our purposes, n is odd and we will demand that $\mathscr{L}$ is symmetric, so the following lemma (proved at the end of the section) holds.

Lemma 5. *Let $\tilde{u} : \tilde{A} \to \tilde{A}'$ be an isogeny of abelian varieties which is the quotient by a maximal isotropic subgroup of $\tilde{A}[n]$ with respect to the Weil pairing induced by a choice of symmetric theta divisor $\tilde{\Theta}$ on $\tilde{A}$. There are $|\tilde{u}(\tilde{A}[n])(F)|$ choices of a theta divisor $\tilde{\Theta}'$ satisfying $\tilde{u}^*\tilde{\Theta}'$ is linearly equivalent to $n\tilde{\Theta}$ (the choices of $\tilde{\Theta}'$ differ by translates of the elements of $\tilde{u}(\tilde{A}[n])(F)$). If n is odd, then there is a unique choice of theta divisor $\tilde{\Theta}'$ making it symmetric.*

If Θ and Θ' are the symmetric theta divisors attached to $\mathscr{L}$ and $\mathscr{L}'$, respectively (so are also defined over F), then $u^*\Theta' - n\Theta$ is linearly equivalent to zero, hence there is a function $\Phi_{u,\mathscr{L},\mathscr{L}'}$ on A defined over F which satisfies

$$(\Phi_{u,\mathscr{L},\mathscr{L}'}) = u^*\Theta' - n\Theta.$$

In this circumstance we will say that Θ and Θ' are compatible divisors. Note that this condition defines $\Phi_{u,\mathscr{L},\mathscr{L}'}$ up to a multiplicative constant. This notion is a bit too general for our purposes as it does not specify the constant. We will add the addtional data of a function g representing Θ in a neighborhood of the identity and a function g' with the analogous properties on A', both defined over F.

We then define the division polynomial $\Phi_{u,g,g'}$ (defined over F) by the equations

$$(\Phi_{u,g,g'}) = u^*\Theta' - n\Theta \tag{2.1}$$

$$1 = \Phi_{u,g,g'} \cdot \frac{g^n}{u^*g'}(0_A). \tag{2.2}$$

The definitions of g and g' ensure the right hand side of (2) is finite and nonzero. Given these choices, we finally have a uniquely defined function on A. In fact, the function $\Phi_{u,g,g'}$ actually only depends on the classes of g and g' modulo the squares of the maximal ideals of the stalks at the identities of A and A' (i.e., multiplying g by a function h which does not vanish in a neighborhood of 0_A and satisfies $h(0_A) = 1$ implies $\Phi_{u,g,g'} = \Phi_{u,gh,g'}$ and similarly for g'). In dimension one, if we take Θ and Θ' to be the respective origins, since any subgroup of an elliptic curve of order n is a maximal isotropic subgroup of the n-torsion, this definition recovers the division polynomials defined by Mazur and Tate (up to an explicit isomorphism **in dimension one** between the tangent and cotangent spaces at the identity).

Multiplying the g, g' by constants, we have

$$\Phi_{u,cg,c'g'} = c'c^{-n}\Phi_{u,g,g'}.$$

These division polynomials satisfy a certain "chain rule."

Proposition 6. *(chain rule) Let $u : A \to A'$ be a maximal isotropic quotient of $A[n]$ and $u' : A' \to A''$ be a maximal isotropic quotient of $A'[n']$, with compatible symmetric theta divisors $\Theta, \Theta', \Theta''$ locally represented in neighborhoods of the origin by g, g', g''. Then*

$$\Phi_{u'\circ u,g,g''} = u^*\Phi_{u',g',g''} \cdot \left(\Phi_{u,g,g'}\right)^{n'}.$$

Proof. Note first that $(u'\circ u)^*\mathcal{L}(\Theta'') = u^*u'^*\mathcal{L}(\Theta'') \cong u^*\mathcal{L}(\Theta')^{n'} \cong \mathcal{L}(\Theta)^{nn'}$. Then ([46] Lemma 2 of Section 23) along with the fact that $\mathcal{L}(\Theta'')$ defines a principal polarization imply that $u'\circ u : A \to A''$

is a maximal isotropic quotient of $A[nn']$ under the Weil pairing induced by $\mathcal{L}(\Theta)^{nn'}$, and thus $u' \circ u$ has a division polynomial.

We need only check that the right hand side of the equation satisfies conditions (1) and (2) for $u' \circ u$, Θ, Θ'', g and g''. We have the following calculations

$$\begin{aligned}\left(u^*\Phi_{u',g',g''} \cdot \left(\Phi_{u,g,g'}\right)^{n'}\right) &= u^*\left(u'^*\Theta'' - n'\Theta'\right) + n'\left(u^*\Theta' - n\Theta\right)\\ &= (u' \circ u)^*\Theta'' - n'u^*\Theta' + n'u^*\Theta' - nn'\Theta\\ &= (u' \circ u)^*\Theta'' - nn'\Theta\\ &= \left(\Phi_{u'\circ u,g,g''}\right)\end{aligned}$$

and

$$\begin{aligned}u^*\Phi_{u',g',g''} \cdot \left(\Phi_{u,g,g'}\right)^{n'} \cdot \frac{g^{nn'}}{(u' \circ u)^* g''}(0_A) &= u^*\Phi_{u',g',g''} \cdot \left(\Phi_{u,g,g'}\right)^{n'} \cdot \frac{u^* g'^{n'}}{(u' \circ u)^* g''}\frac{g^{nn'}}{u^* g'^{n'}}(0_A)\\ &= u^*\left(\Phi_{u',g',g''} \cdot \frac{g'^{n'}}{u'^* g''}\right) \cdot \left(\Phi_{u,g,g'} \cdot \frac{g^n}{u^* g'}\right)^{n'}(0_A)\\ &= \left(\Phi_{u',g',g''} \cdot \frac{g'^{n'}}{u'^* g''}(u(0_A))\right) \cdot \left(\Phi_{u,g,g'} \cdot \frac{g^n}{u^* g'}(0_A)\right)^{n'}\\ &= 1 \cdot 1^{n'} = 1.\end{aligned}$$

Note that line 4 above follows from line 3 because $u(0_A) = 0_{A'}$. □

We finish the section with the promised proof of the symmetry lemma.

Proof of Lemma 5. Note that for maximally isotropic quotients, some choice of $\tilde{\Theta}'$ exists. In particular, $\varphi_{\mathcal{L}(\Theta')} : \tilde{A}' \to \hat{\tilde{A}}'$ has degree one (so is an isomorphism, hence surjective on F points) as $\tilde{\Theta}'$ is a theta divisor. The first part is then the content of Corollary 3 in Section 2.1.2.

If n is odd, then we have

$$\tilde{u}^*[-1]^*\tilde{\Theta}' \cong [-1]^*\tilde{u}^*\tilde{\Theta}' \cong [-1]^*n\tilde{\Theta} \cong n([-1]^*\tilde{\Theta}) \cong n\tilde{\Theta} \cong u^*\tilde{\Theta}'.$$

By Corollary 3, there must be some $P \in \tilde{u}(\ker \varphi_{n\cdot\tilde{\Theta}})(F) = \tilde{u}(\ker[n]_{\tilde{A}})(F)$ such that $[-1]^*\tilde{\Theta}' \cong T_P^*\tilde{\Theta}'$. If $x \in \tilde{A}'$, then

$$[-1]^*T_x^*\tilde{\Theta}' \cong T_{-x}^*[-1]^*\tilde{\Theta}' \cong T_{-x}^*T_P^*\tilde{\Theta}'.$$

Hence $T_x^*\tilde{\Theta}'$ is symmetric if and only if $T_x^*\tilde{\Theta}' \sim T_{P-x}^*\tilde{\Theta}'$ which is the same as that $\tilde{\Theta}' \sim T_{P-2x}^*\tilde{\Theta}'$. This is equivalent to $P-2x$ lying in $\ker(\varphi_{\tilde{\Theta}'})$, which is the trivial group. That is to say $P=2x$ or that $x \in [2]^{-1}(P)$. On the other hand, since n was odd, $\tilde{u}(\tilde{A}[n])(F)$ is an odd order group, hence uniquely 2 divisible. We get a unique element $\frac{P}{2} \in \tilde{u}(\tilde{A}[n])(F)$ satisfying $T_{\frac{P}{2}}^*\tilde{\Theta}'$ is symmetric. By Corollary 3, we can take this as our new $\tilde{\Theta}'$. □

Remark: the requirements that n be odd and the line bundles be symmetric can be dropped from the section's discussion, at the cost of possibly requiring a field extension to define the Φ.

2.2.2 Towers

Now that we have a general theory of division polynomials, we must introduce the isogenies we will want to study. We first introduce the assumptions to be held for the remainder of the chapter. Let p be an odd prime. Let K be a p-adic field with ring of integers R, uniformizer π (dividing p) and residue field k. Let A be an abelian variety of (good) ordinary reduction of dimension g defined over K with a choice of K-rational symmetric theta divisor Θ and $\mathcal{A}$ the associated abelian scheme over R. We will refer to the generic fiber of a scheme over R by a subscript η and the special fiber by a subscript s.

By the ordinary assumption, after a finite unramified extension S of R,

$$\mathcal{A}[p^n] \cong (\mathbb{Z}/p^n\mathbb{Z})^g \times \mu_{p^n}^g.$$

Let $\mathcal{C}_n$ be the closure of $\mathcal{A}[p^n] \cap \mathcal{A}^f$ in $\mathcal{A}$. This is a connected finite flat group scheme of order p^{gn}, the part which is isomorphic to $\mu_{p^n}^g$ over S. We can define quotients $\mathfrak{b}_n : \mathcal{A} \to \mathcal{A}_n = \mathcal{A}/\mathcal{C}_n$. There are then intermediate quotients $\mathfrak{b}_{m,n} : \mathcal{A}_m \to \mathcal{A}_n$ for $m \le n$ satisfying $\mathfrak{b}_{m,n} \circ \mathfrak{b}_m = \mathfrak{b}_n$. When convenient, we will refer to $\mathfrak{b}_n$ by $\mathfrak{b}_{0,n}$. These give a sequence of maps

$$\mathcal{A} = \mathcal{A}_0 \xrightarrow{\mathfrak{b}_1} \mathcal{A}_1 \xrightarrow{\mathfrak{b}_{1,2}} \mathcal{A}_2 \xrightarrow{\mathfrak{b}_{2,3}} \mathcal{A}_3 \to \cdots.$$

We want, in some sense, the tower dual to this. The image of $\mathcal{A}[p^n]$ under $\mathfrak{b}_n$ is an étale finite flat group scheme of $\mathcal{A}_n$ of order p^{ng}, the quotient by which gives us an isogeny $\mathfrak{a}_n : \mathcal{A}_n \to \mathcal{A}$ such that $\mathfrak{a}_n \circ \mathfrak{b}_n = [p^n]_{\mathcal{A}}$ (note that this also implies that $\mathfrak{b}_n \circ \mathfrak{a}_n = [p^n]_{\mathcal{A}_n}$). The upshot is we have a collection of étale covers

$$\mathcal{A} \xleftarrow{\mathfrak{a}_1} \mathcal{A}_1 \xleftarrow{\mathfrak{a}_{2,1}} \mathcal{A}_2 \xleftarrow{\mathfrak{a}_{3,2}} \mathcal{A}_3 \leftarrow \cdots .$$

Taking the generic fibers, we get a tower of isogenies

$$A \xleftarrow{a_1} A_1 \xleftarrow{a_{2,1}} A_2 \xleftarrow{a_{3,2}} A_3 \leftarrow \cdots .$$

We would like to attach division polynomials to the various a_n. To do so, we will select suitable symmetric theta divisors on the A_n which are compatible with Θ and the a_n (in the sense that $a_n^*\Theta \sim p^n \cdot \Theta_n$), along with choices of functions g_n representing Θ_n on some neighborhood containing the origin. To this end, we need the following.

Lemma 7. *The subgroup $C_n = A[p^n] \cap \mathcal{A}^f$ inside $A[p^n]$ is a maximal isotropic subgroup with respect to the Weil pairing $e^{p^n\Theta}$ induced by $p^n\Theta$.*

Proof. We offer two proofs.

(First proof) We will assume K is perfect. Note that by the formulae on [46] p.228, the Weil pairings are compatible in the sense that the following diagram commutes

$$\begin{tikzcd}
A[p^n] \times A[p^n] \arrow[r, "e^{p^n\Theta}"] \arrow[d, "{[p]}"'] & \mu_{p^n} \arrow[d, "{[p]}"] \\
A[p^{n-1}] \times A[p^{n-1}] \arrow[r, "e^{p^{n-1}\Theta}"] & \mu_{p^{n-1}}
\end{tikzcd}$$

which means that the pairings induce an antisymmetric Galois equivariant bilinear map $e : T_A \times T_A \to T_{\mathbb{G}_m}$ on the Tate module of A. This restricts to an antisymmetric Galois equivariant bilinear map $e : \varprojlim C_n \times \varprojlim C_n \to T_{\mathbb{G}_m}$. On some unramified extension L of K, we have that $\mathcal{A}^f \cong (\mathbb{G}_m^g)^f$, so after base change to L, we get $e : T_{\mathbb{G}_m^g} \times T_{\mathbb{G}_m^g} \to T_{\mathbb{G}_m}$ as Galois modules. Since K is a perfect local field, it does not contain all of its p^n-th roots of unity. As L is unramified over K, it contains no p-power roots of unity K does not possess, so $T_{\mathbb{G}_m}$ is a nontrivial Galois module over L. That is, we have an action of $\mathrm{Gal}(L(\mu_{p^\infty})/L)$ on $T_{\mathbb{G}_m}$ which is nontrivial. This amounts to a nontrivial continuous homomorphism $\chi : \mathrm{Gal}(L(\mu_{p^\infty})/L) \to \mathbb{Z}_p^*$.

Let τ be an element of $\mathrm{Gal}(L(\mu_{p^\infty})/L)$ and u and v be elements of $T_{\mathbb{G}_m}$. We have

$$e(u,v)^{\chi(\tau)} = \tau e(u,v) = e(\tau u, \tau v) = e(u^{\chi(\tau)}, v^{\chi(\tau)}) = e(u,v)^{\chi(\tau)^2}.$$

But then $1 = e(u,v)^{\chi(\tau)(\chi(\tau)-1)}$ and since $\chi(\tau)$ is in $\mathbb{Z}_p^*$, we get $1 = e(u,v)^{(\chi(\tau)-1)}$. Then if $e(u,v)$ is not 1 in $T_{\mathbb{G}_m}$, it must be that $\chi(\tau) = 1$ for every τ. But χ is not identically trivial, so $e(u,v) = 1$. This says that e restricted to $\varprojlim C_n \times \varprojlim C_n$ sends everything to 1, hence $e^{p^n\Theta}$ restricted to $C_n \times C_n$ is trivial, i.e., C_n is an isotropic subgroup of $A[p^n]$. Yet the order of C_n is p^n, which is the maximal possible size of an isotropic subgroup.

(Second proof) Work at the level of the Néron model. The pairing restricted to $\mathcal{C}_n \times \mathcal{C}_n \to \mu_{p^n}$ is the same as a group morphism $\mathcal{C}_n \to \mathcal{C}_n^\vee$, to the dual of $\mathcal{C}_n$, defined on schematic points by $x \mapsto (y \mapsto e^{p^n\Theta}(x,y))$. At the same time, the Cartier dual of $\mathcal{C}_n$ is an étale group since after base extension, $\mathcal{C}_n \cong \mu_{p^n}^g$. However, since $\mathcal{C}_n$ is connected, the only morphisms to $\mathcal{C}_n^\vee$ are constant. Hence the pairing $\mathcal{C}_n \times \mathcal{C}_n \to \mu_{p^n}$ must be identically trivial, forcing C_n to be an isotropic subgroup of $A[p^n]$. It is also the maximal possible size for such a subgroup, hence is maximal isotropic.

□

Let Θ_n be the symmetric theta divisor obtained by taking $\tilde{A} = A$, $\tilde{u} = b_n$ and $\tilde{\Theta} = \Theta$ in Lemma 5. Then $b_n(A[p^n])$ is a maximal isotropic subgroup of $A_n[p^n]$ with quotient map a_n, so we may again apply the lemma with $\tilde{A} = A_n$, $\tilde{u} = a_n$ and $\tilde{\Theta} = \Theta_n$, getting an apparently new symmetric divisor Θ' on A. We find $[p^n]^*\Theta' \sim b_n^* a_n^* \Theta' \sim b_n^* p^n \Theta_n \sim p^{2n}\Theta$ but also $[p^n]^*\Theta \sim p^{2n}\Theta$. By the lemma where $\tilde{A} = A$, $\tilde{u} = [p^n]$ and $\tilde{\Theta} = \Theta$, since $A[p^n]$ is a maximal isotropic subgroup of $A[p^{2n}]$, A is a maximal isotropic quotient of itself. Hence $\tilde{\Theta} = \Theta$, since Θ is the unique symmetric divisor with $[p^n]^*\Theta \sim p^{2n}\Theta$, and so we must have $\Theta = \Theta'$. Similar arguments show that $a_{n,m}^*\Theta_m \sim p^{n-m}\Theta_n$ and $b_{m,n}^*\Theta_n \sim p^{n-m}\Theta_m$.

Now we have not only a tower of abelian varieties $A \xleftarrow{a_1} A_1 \xleftarrow{a_{2,1}} A_2 \leftarrow \cdots$ but also corresponding choices of symmetric theta divisors Θ_n. The next step is to find local functions g_n representing the various Θ_n at neighborhoods of the origin of each of the A_n to use to define division polynomials with divisors $a_n^*\Theta - p^n\Theta_n$. In particular, we will want these division polynomials (a priori defined over K) to be defined over R, so we will enrich the above divisors with an R structure.

Lemma 8. *If D is a Weil divisor on A (defined over K), then the following hold:*

(a) D extends uniquely to a horizontal Weil divisor for any projective model of A over R

(b) D is also represented as a relative Cartier divisor on the projective model over R. That is to say, there is an open cover $\mathcal{U}$ of open sets U such that each U is the complement of $V(f_1, \ldots, f_{r_U})$ for some set of f_i, where each f_i is defined over R, and such that on U there exist holomorphic functions g and h defined over R such that D agrees with $\left(\frac{g}{h}\right)$.

Proof. (a) Since A is projective, it is given by a homogenous ideal $I = (f_1, \ldots, f_s)$ inside $\mathbb{P}^r_K$. After multiplying each of the elements of I by an appropriate power of π, they are all defined over R and nonvanishing over k. This is the closure of A in $\mathbb{P}^r_R$. Since D is closed in A, it is also closed in $\mathbb{P}^r_K$, so it is given by some homogenous ideal $J \supseteq I$. After doing the same procedure to J, we get an ideal that cuts out a codimension one subset of A defined over R. As a scheme, this is the closure of the image of D under the map $A \hookrightarrow \mathbb{P}^r_R$ (See [42] Section II.8).

To see that D is horizontal over R (i.e., no component vanishes modulo π), it suffices to consider the case of an irreducible component. If an irreducible component were vertical, the dimension of its specialization would be strictly less than the dimension of D over K, which is impossible per [42] Corollary of Normalization Lemma, Section II.8.

(b) If D is given by a Cartier divisor $(g_U)_U$ for some open cover $\bigcup U = A$, then each of the representing meromorphic functions g_U is a quotient of homogenous polynomials of equal degree $\frac{\alpha_U}{\beta_U}$ defined over K. There is a unique power of π making $\pi^{r_U}\frac{\alpha_U}{\beta_U}$ defined over R. We can thus renormalize the $g_U = \frac{\alpha_U}{\beta_U}$ to be defined over R. Having done so, on the overlap $U \cap V$, $g_U = g_V \cdot u$ for some invertible function on $U \cap V$, a priori defined over K. But since $u = \frac{\alpha_U}{\beta_U} \cdot \frac{\beta_V}{\alpha_V}$ and the right hand side has already been normalized to be defined over R, so too must be u.

Note an open set U is the complement of $V(I)$ for some homogeneous ideal I. Each of these homogenous elements can be normalized in the same fashion to be defined over R, and so U extends to an open set defined over R which is the complement of $V(I_R)$. Hence D is defined by a Cartier divisor with all meromorphic functions and transition maps defined over R. □

For our purposes, we need only a single open set U_n on each A_n containing the identity, but with one further stipulation. We will require each of the U_n to contain the kernel of reduction $\mathcal{A}_n^f$, i.e., U_n should contain every point of A which reduces to the identity on $\mathcal{A}_s$. We can always do this, as we can take any hyperplane in $\mathbb{P}_k^r$ which misses the identity and take any lift to $\mathbb{P}_R^r$ and use the complement of this lift in A.

In light of the above discussion, each of the Θ_n is defined locally in some neighborhood U_n of the kernel of reduction by a meromorphic function g_n defined over R. We will fix such an abritrarily selected collection now.

With these choices, we define division polynomials $\phi_n = \Phi_{a_n,g_n,g}$ over R.

Lemma 9. *If f is a global meromorphic function on A (defined over K), then the following hold:*

(a) There is a unique power t of π such that $\pi^t \cdot f$ is defined over R and nonvanishing over k.

(b) Let Q be a point of $A(K)$ with f as in (a) defined over K. As in Lemma 8 (b), there is some neighborhood U of the entire set of points in $A(K)$ reducing to $\tilde{Q} \in A(k)$, where U is the complement of a closed set in schemes over R, such that the divisor (f) is represented by $\frac{g}{h}$, where both g and h are defined over R. For such a representative, if $|f \cdot \frac{h}{g}(Q)|_\pi = 1$, then f must have been defined over R.

In particular, if on some neighborhood U of the kernel of reduction $\mathcal{A}^f(R)$, the divisor (f) is represented by $\frac{g}{h}$ with g and h defined over R, and if $|f \cdot \frac{h}{g}(0)|_\pi = 1$, then f must be defined over R.

Proof. (a) As in the last proof, since A is projective, it is given by a homogenous ideal $I = (f_1, \ldots, f_s)$ inside $\mathbb{P}_K^r$. Then f is represented as $\frac{g}{h}$ where both g, h are homogeneous polynomials of the same degree in $K[x_0, \ldots, x_r]$, and we can assume they both have coefficients in R. Let a, b be the maximal power of π dividing the coefficients of g, h respectively, then $\frac{\pi^{-a}}{\pi^{-b}}\frac{g}{h} = \pi^{b-a}f$ has the desired property. Note that since the special fiber is irreducible, multiplying or dividing f by π will either make the function identically zero over k or nowhere defined over k.

(b) By construction, the support of the divisor $(f \cdot \frac{h}{g})$ has no component going through the reduction of Q on $\mathcal{A}_s$. But by (a), $f \cdot \frac{h}{g}$ can be defined over R by replacing f by some $f' = \pi^r f$. Hence $f'\frac{h}{g}$ can be taken modulo π, giving a function $\widetilde{f'\frac{h}{g}}$ on $\mathcal{A}_s$ where $\widetilde{f'\frac{h}{g}}(\tilde{Q})$ is finite and nonzero. Hence $|f'\frac{h}{g}(Q)|_\pi = 1$. So by the uniqueness result in (a), $r = 0$ and $f' = f$.

□

In all of our applications, we will take Q above to be 0_A, so the points with a common reduction are exactly the R points of $\mathcal{A}^f$.

Note that since $\mathcal{A} \to \operatorname{Spec} R$ is smooth, then for any section s, the completion $\hat{\mathcal{O}}_{\mathcal{A},s} \cong R[[t_1, \ldots, t_g]]$ for any collection $t_1, \ldots, t_g$ of local parameters at s defined over R. This is Exercise 6.2.1 in [26]. Hence, if f is regular at a point P in $\mathcal{A}(R)$, then by Lemma 9 (b), for some r, the restriction of $\pi^r \cdot f$ to $\hat{\mathcal{O}}_{\mathcal{A},P}$ is a power series in the t_i with coefficients in R.

Since $a_n : A_n \to A$ came from a map of Neron models $\mathcal{A}_n \to \mathcal{A}$ it is defined over R. So if g is a meromorphic function defined over R on A such that $(g)|_U = \Theta|_U$, then $a_n^* g$ is also defined over R (i.e., it is given by $\mathfrak{a}_n^* g$) and satisfies $(a_n^* g)|_{a_n^{-1}U} = a_n^*\Theta|_{a_n^{-1}U}$. At the same time, if U contains the kernel of reduction A^f, then $a_n^{-1}U$ contains all points of A_n mapping to the kernel of reduction under a_n, so in particular it contains A_n^f (any element of A_n^f maps via reduction to $\tilde{0}$, hence to $\tilde{0}$ under a_n). In particular, since the g_n are defined over R on open sets containing $\mathcal{A}^f$, we have the ϕ_n are also defined over R.

The entire discussion of this section, given global choices of g_n and U_n, follows mutatis mutandi for the isogenies $a_{n,m} : A_n \to A_m$ for $n > m$, giving division polynomials $\phi_{n,m} = \Phi_{a_{n,m}, g_n, g_m}$ defined over R.

We include a convergence lemma.

Lemma 10. *Let $\mathfrak{m}$ be the ideal generated by $\pi, t_1, \ldots, t_g$ in $R[[t_1, \ldots, t_g]]$.*

(a) For m in $\mathfrak{m}$, the element $(1+m)^{p^n}$ is in $1+\mathfrak{m}^n$.

(b) If $\{f_n\}$ is a sequence of elements in $1+\mathfrak{m}^n$, the f_n converge in $R[[t_1, \ldots, t_g]]$ to 1.

Proof. (a) Suppose m_ℓ is in $\mathfrak{m}^\ell$, then binomial theorem yields

$$(1+m_\ell)^p = 1 + \sum_{i=1}^{p} \binom{p}{i} m_\ell^i$$

where $\binom{p}{i}$ is in $\mathfrak{m}$ unless $i = p$, in which case m_ℓ^p in in $\mathfrak{m}^{p\ell}$. Thus we have that each term in $\sum_{i=1}^{p} \binom{p}{i} m_\ell^i$ is in $\mathfrak{m}^{\ell+1}$. By induction, we have $(1+m)^{p^n}$ is in $1+\mathfrak{m}^n$.

(b) We have $f_{n_1} - f_{n_2}$ is in $\mathfrak{m}^{\min\{n_1,n_2\}}$. Since $\bigcap \mathfrak{m}^n = 0$, the convergence follows.

□

2.2.3 Sigma functions

We use the division polynomials defined for the isogenies in the tower from the previous section to define approximations to the σ function.

We define approximations to σ by $\sigma_n = \phi_n \cdot g_n^{p^n}$. Since the right hand side is defined over R, so is the left hand side. In particular, the right hand side is equal to g times a unit power series with constant coefficient 1 in $\hat{\mathcal{O}}_{\mathcal{A}_n,0}$. Since the $\mathfrak{a}_n$ are étale, they induce isomorphisms of formal groups $\mathcal{A}^f \cong \mathcal{A}_n^f$. Under this identification, we can view the σ_n as living on the common space $\mathcal{A}^f$. Alternatively, we can think of defining a set of local parameters to the identity section on $\mathcal{A}$ given by $t_1, \ldots, t_g$, then the pullbacks of the t_i under $\mathfrak{a}_n$ give a set of local parameters to the identity section on $\mathcal{A}_n$, which in turn gives an explicit identification $\hat{\mathcal{O}}_{\mathcal{A},0} \to \hat{\mathcal{O}}_{\mathcal{A}_n,0}$ by identifying the coefficients of the monomials in t_i and those in $\mathfrak{a}_n^* t_i$.

Theorem 11. *Let A be an abelian variety of good ordinary reduction over K with Néron model $\mathcal{A}$, along with a choice of symmetric theta divisor Θ with local equation $g = 0$ over R in a neighborhood of the identity on $\mathcal{A}_s$. With Θ_n and g_n as defined previously, the limit $\lim\limits_{n\to\infty} \sigma_n$ exists as a power* *series in $\hat{\mathcal{O}}_{\mathcal{A},0}$, and hence as a function on the kernel of reduction of $\mathcal{A}$, and is independent of the choices of g_n.*

Proof. We have

$$\begin{aligned}
\sigma_n &= g_n^{p^n} \cdot \phi_n \\
&= g_n^{p^n} \cdot a^*_{n,n-1}\phi_{n-1} \cdot (\phi_{n,n-1})^{p^{n-1}} && \text{by Proposition 6} \\
&= a^*_{n,n-1}\phi_{n-1} \cdot (g_n^p \cdot \phi_{n,n-1})^{p^{n-1}} \\
&= a^*_{n,n-1}\phi_{n-1} \cdot a^*_{n,n-1} g_{n-1}^{p^{n-1}} \cdot \left(\frac{g_n^p}{a^*_{n,n-1} g_{n-1}} \cdot \phi_{n,n-1} \right)^{p^{n-1}} \\
&= a^*_{n,n-1} \left(g_{n-1}^{p^{n-1}} \cdot \phi_{n-1} \right) \cdot \left(\frac{g_n^p}{a^*_{n,n-1} g_{n-1}} \cdot \phi_{n,n-1} \right)^{p^{n-1}} \\
&= a^*_{n,n-1}\sigma_{n-1} \cdot \left(\frac{g_n^p}{a^*_{n,n-1} g_{n-1}} \cdot \phi_{n,n-1} \right)^{p^{n-1}} && \text{by Proposition 6}
\end{aligned}$$

since $\frac{g_n^p}{a^*_{n,n-1} g_{n-1}} \cdot \phi_{n,n-1}$ is a power series with constant term 1, its p^{n-1}-st power is in $1 + \mathfrak{m}_n^{n-1}$ by Lemma 10 (a). Recall $a^*_{n,n-1}\sigma_{n-1} = \sigma_{n-1}$ under the identification in $\hat{\mathcal{O}}_{\mathcal{A},0}$, and $1 + \mathfrak{m}_n^{n-1}$ is identified with $1 + \mathfrak{m}^{n-1}$, so by Lemma 10 (b) the σ_n tend to a limit in $\hat{\mathcal{O}}_{\mathcal{A},0}$.

Now note that changing g_n by a constant c changes ϕ_n by a factor of c^{-p^n} and hence leaves σ_n invariant. Changing g_n by an element of $1 + \mathfrak{m}_n$ changes σ_n by a factor in $(1 + \mathfrak{m})^{p^n}$ after our identification, hence leaving the limit unchanged. □

We define σ to be the function achieved by this limit. A priori σ depends on the choice of g. We denote this dependence by σ_g. For a constant c in R^*, changing g to cg does not affect the g_n for $n \geq 1$ (as g_n was determined only by Θ_n), hence the $\phi_{n,n-1}$ are unchanged for $n > 1$ and $\phi_{n,cg} = \Phi_{a_n,g_n,cg} = c \cdot \Phi_{a_n,g_n,g} = c \cdot \phi_{n,g}$. Then $\sigma_{n,g} = c \cdot \sigma_{n,g}$, so after taking limits we have $\sigma_{cg} = c\sigma_g$. For u a power series over R with constant term 1, under $g \mapsto ug$ there is no change to the g_n for $n \geq 1$ nor any change to the $\phi_{n,m}$ for all m, n, hence $\sigma_{ug} = \sigma_g$.

Given a collection of local parameters to the origin $t_1, \ldots, t_g$ defined over R on A, σ will be expressed as a series $\sigma = \sum_I \alpha_I t^I$ where the I run over all indices $I \in \mathbb{N}^g$. If Θ contains 0, then

$\alpha_0 = 0$. If Θ does not contain 0 but Θ_s contains 0, then $0 < |\alpha_0| < 1$. If Θ_s does not contain 0, then $|\alpha_0| = 1$. In all cases, the constant term will agree with $g(0_A)$. More precisely, by the construction it is apparent that σ is expressed as $g \cdot u$ for a power series u in $t_1, \ldots, t_g$ with coefficients in R and constant coefficient 1.

Remark: since $\sigma_{cg} = c\sigma_g$ for any c in R^*, we can extend our construction in the following way: if g, defined over K, represents Θ on a neighborhood of the origin containing $\mathcal{A}^f$ and t is the power of π appearing in Lemma 9(a), then $\sigma_g = \pi^{-t}\sigma_{\pi^t g}$. In this case, σ_g will be an element of $\pi^{-t}\hat{\mathcal{O}}_{\mathcal{A},0}$. In the notation of the previous paragraph, we still have $\sigma_g(0_A) = \alpha_0$ and $\sigma_g = g \cdot u$.

2.3 Properties of σ functions

We now wish to establish some of the basic properties of σ.

The first thing we might hope that in addition to σ vanishing along $\Theta \cap A^f$, σ is even or odd depending on whether Θ is even or odd.

Proposition 12. *The function σ is either even or odd depending on whether Θ is even or odd.*

Proof. We wish to compute $\sigma \circ [-1]$. Since the divisor of ϕ_n is symmetric, we have $[-1]^*\phi_n = \pm\phi_n$. Hence we need to determine only the sign. Let's consider the normalization of ϕ_n. Note that since Θ_n is symmetric, $[-1]^*g_n$ still represents Θ_n on some neighborhood of the origin, hence we can consider its role in defining the σ_n. By construction,

$$\phi_n \cdot \frac{g_n^{p^n}}{a_n^* g}(0) = \Phi_{a_n \cdot g_n, g} \cdot \frac{g_n^{p^n}}{a_n^* g}(0) = 1$$

so then (using that isogenies commute with $[-1]$)

$$1 = \left(\phi_n \cdot \frac{g_n^{p^n}}{a_n^* g}\right)(0) = \left(\phi_n \cdot \frac{g_n^{p^n}}{a_n^* g}\right)([-1]0) = [-1]^*\phi_n \cdot \frac{[-1]^* g_n^{p^n}}{a_n^*[-1]^* g}(0).$$

Recalling the definition of division polynomials, we get $[-1]^*\phi_n = [-1]^*\Phi_{a_n,g_n,g} = \Phi_{a_n,[-1]^*g_n,[-1]^*g}$. Because the choice of g_n did not affect the limit $g_n^{p^n}\Phi_{a_n,g_n,g} \to \sigma_g$, we have

$$[-1]^*\sigma_g = \sigma_{[-1]^*g}.$$

On the other hand, $[-1]^*g = u \cdot g$ for some power series u with constant coefficient $c = 1$ if Θ is even and $c = -1$ if Θ is odd (see Section 2.1.2.2). We get that $[-1]^*\sigma_g = \sigma_{ug} = c\sigma_g$ (see the discussion following Theorem 11).

□

We can further find that the ϕ_n are all even functions. First we need the following.

Lemma 13. *Let $f : B \to B^{(p)}$ be the Frobenius morphism, where B is an abelian variety defined over k. If D is a symmetric theta divisor on B and D' is the unique symmetric theta divisor on $B^{(p)}$ such that $pD \sim f^*D'$ promised in Lemma 5, then D and D' are both even or both odd.*

Proof. Let $(g_U)_U$ be the Cartier divisor attached to D. Let $g^{(p)}$ be the function defined by taking the coefficients of g to the power p. Then $f^*g^{(p)} = g^p$. In particular, $D^{(p)}$ is given as a Cartier divisor by $(g_U^{(p)})_{f(U)}$ and pulling back by f, we have $f^*D^{(p)}$ is given by $(f^*g_U^{(p)})_U = (g_U^p)_U$, or that $f^*D^{(p)} = p \cdot D$. On the level of line bundles, $f^*\mathcal{L}(D^{(p)}) = \mathcal{L}(D)^p$, so by the discussion in [46] p. 231-234, f must be a maximal isotropic quotient of the p-torsion of B. On the other hand, if $[-1]^*D = D$, then $[-1]^*D^{(p)} = D^{(p)}$ so $D^{(p)}$ is also symmetric. By the uniqueness in Lemma 5, $D' = D^{(p)}$.

Note that if U contains the identity and $[-1]^*g_U = g_U \cdot u$ on $U \cap [-1]U$, then $[-1]^*g_U^{(p)} = g_U^{(p)} \cdot u^{(p)}$ on $f(U \cap [-1]U)$. In particular, $u^{(p)}(0) = u(0)^p$ and as $u(0) = \pm 1$ and p is odd, we have $u^{(p)}(0) = u(0)$, hence D and D' are either both even or both odd. □

Corollary 14. *The symmetric theta divisors Θ_n are either all even or all odd.*

Proof. We show that if Θ_n is even (resp. odd) then so is Θ_{n+1}. The pullback to the special fiber of $\mathfrak{b}_{n,n+1}$ has the same kernel as the Frobenius isogeny $\mathrm{Frob} : \mathcal{A}_{n,s} \to \mathcal{A}_{n,s}^{(p)}$ (there is only one connected subgroupscheme of $\mathcal{A}_{n,s}[p]$ of order p^g) and hence there is an isomorphism $f : \mathcal{A}_{n+1,s} \to \mathcal{A}_{n,s}^{(p)}$ such that $\mathrm{Frob} = f \circ \mathfrak{b}_{n,n+1}$. By the uniqueness in Lemma 5, $\Theta_{n+1,s} = f^*\Theta'_{n,s}$. Hence by Lemma 13, the special fibers of Θ_n and Θ_{n+1} are both even (resp. odd). Since this is determined by looking at the constant coefficient $\frac{[-1]^*g_n}{g_n}$ (which is either 1 or -1), and this is invariant modulo π (since $p \neq 2$), it must also be that Θ_n and Θ_{n+1} are both even (resp. odd). □

Corollary 15. *The division polynomials ϕ_n are even.*

Proof. Since the divisor of ϕ_n is fixed by $[-1]$, the function $\phi_n/[-1]^*\phi_n$ is a nonvanishing function on all of A_n, hence constant. Then by the discussion in Section 2.1.2.2, that constant is either 1 or -1. Write $[-1]^*g = g \cdot u$ and $[-1]^*g_n = g_n \cdot u_n$. We have

$$[-1]^* \frac{a_n^* g}{g_n^{p^n}} = \frac{a_n^* g}{g_n^{p^n}} \cdot \frac{a_n^* u}{u_n^{p^n}}.$$

Note that a_n induces a map $a_n^* : K[[t_1, \ldots, t_g]] \to K[[t_{1,n}, \ldots, t_{g,n}]]$ sending the t_i to power series in $t_{j,n}$ with no constant term, so the constant terms of u' and $a_n^* u'$ are the same. As per the discussion in Section 2.1.2.2, the evenness/oddness of Θ and Θ_n are determined by the constant terms of u and u_n, so they must agree by Corollary 14. Since the constant terms of u, u_n and $a_n^* u$ are all the same, the constant term of $\frac{a_n^* u}{u_n^{p^n}}$ must be 1. □

There are several manipulations of Θ which give rise to meromorphic functions on various powers of A. These should be reflected in the behavior of σ. If D is an effective zero-cycle on A and E a divisor on A, define E_D to be the sum of translates of E by the points in D, $E_D = \sum_{q \in D} T_q^* D$. Similarily, for a meromorphic function f, define f_D to be the product $\prod_{q \in D} T_q^* f$. If $D = D_1 - D_2$ for effective D_1, D_2, we take E_D to mean $E_{D_1} - E_{D_2}$ and $f_D = \frac{f_{D_1}}{f_{D_2}}$.

In much the same way, if f is any ratio of power series $\hat{\mathcal{O}}_{\mathcal{A},0}$ and D any effective 0-cycle supported on the kernel of reduction, we can define f_D as for meromorphic functions by $\prod_{q \in D} T_q^* f$, and if $D = D_1 - D_2$ is a difference of effective 0-cycles, we define $f_D = \frac{f_{D_1}}{f_{D_2}}$.

Note that if D is a sum of K-points of A, then D is supported on R points of $\mathcal{A}$ and hence each of the T_q^* is defined over R and so too must E_D and f_D be (if E and f were defined over R themselves).

Proposition 16. *Let D be a zero-cycle of degree zero supported on $\mathcal{A}^f(R)$ such that the sum of the points (interpreted as points of A) is 0. Then σ_D is the restriction to the kernel of reduction of a rational function ψ on A with divisor Θ_D (i.e., the image of ψ in $\mathcal{O}_{\mathcal{A},0}$).*

Proof. Define D_n to be the restriction of the 0-cycle $a_n^* D$ to the kernel of reduction on A_n. Since a_n^* induces an isomorphism of kernels of reduction of A and A_n, D_n will again be degree zero and sum to 0 in A_n. By the theorem of the square, the divisors Θ_{n,D_n} are principal, so there are rational functions ψ_n on A_n with $(\psi_n) = \Theta_{n,D_n}$. We choose the ψ_n such that $\psi_n / g_{n,D_n}(0) = 1$. Note that the support of g_n intersected with the kernel of reduction is Θ_n intersected with the kernel of reduction, so for q in D_n the support of $T_q^* g_n$ intersected with the kernel of reduction is exactly $T_q^* \Theta_n$ intersected with the kernel of reduction. By Lemma 9, since the g_n are defined over R, we have that $\psi_n = g_{n,D_n} \cdot u_n$ for a power series with coefficients in R and unit term equal to one. We compute

$$\begin{aligned}
(\phi_{n,D_n}) &= (\phi_n)_{D_n} \\
&= \left(a_n^{-1}\Theta - p^n \Theta_n\right)_{D_n} \\
&= a_n^{-1}\left(\Theta_D\right) - p^n\left(\Theta_{n,D_n}\right) \\
&= a_n^{-1}(\psi_0) - p^n(\psi_n).
\end{aligned}$$

Hence there must be constants c_n such that $\phi_{n,D_n} = c_n \dfrac{a_n^* \psi_0}{\psi_n^{p^n}}$. Then we have

$$\begin{aligned}
c_n \cdot a_n^*(\psi_0) &= \phi_{n,D_n} \cdot \psi_n^{p^n} \\
&= g_{n,D_n}^{p^n} \cdot \phi_{n,D_n} \cdot \left(\frac{\psi_n}{g_{n,D_n}}\right)^{p^n} \\
&= \left(g_n^{p^n} \phi_n\right)_{D_n} \left(\frac{\psi_n}{g_{n,D_n}}\right)^{p^n} \\
&= \left(\sigma_{n,D_n}\right)\left(u_n\right)^{p^n}.
\end{aligned}$$

Restricting to the kernels of reduction, since u_n has constant term one, the right hand side converges to σ_D. Thus the left hand side must converge, i.e., the $c_n \to c$ for some c. This gives us $\sigma_D = c\psi_0$.

□

Consider the four maps $m, s, p_1, p_2 : A \times A \to A$ defined by $m(u,v) = u + v$, $s(u,v) = u - v$, $p_1(u,v) = u$ and $p_2(u,v) = v$, where we use $+$ for the group law on $\mathcal{A}^f(R)$.

Proposition 17. *Let u, v be in $\mathcal{A}^f(R)$. The function*

$$\frac{\sigma(u+v)\sigma(u-v)}{\sigma(u)^2\sigma(v)^2}$$

is the restriction to the kernel of reduction of a rational function on $A \times A$ with divisor

$$m^*\Theta + s^*\Theta - 2p_1^*\Theta - 2p_2^*\Theta.$$

Proof. First note there is a function on $A \times A$ with the prescribed divisor by the Theorem of the Square. Let ψ be a function on $A \times A$ with the desired divisor and (u, v) be a point on $\mathcal{A}^f \times \mathcal{A}^f$. By Proposition 16 and the zero-cycle $(v) + (-v) - 2(0)$, there is a constant $\delta_2(v)$ such that $\psi(u, v) = \delta_2(v) \cdot \frac{\sigma(u+v)\sigma(u-v)}{\sigma(u)^2\sigma(v)^2}$. By Proposition 12 we have $\sigma(-P) = \pm\sigma(P)$ so we get $\frac{\sigma(u+v)\sigma(u-v)}{\sigma(u)^2\sigma(v)^2} = \pm\frac{\sigma(v+u)\sigma(v-u)}{\sigma(v)^2\sigma(u)^2}$, hence again using the proposition and the zero-cycle $(u)+(-u)-2(0)$, there is a constant $\delta_1(u)$ such that $\psi(u, v) = \delta_1(u) \cdot \frac{\sigma(u+v)\sigma(u-v)}{\sigma(u)^2\sigma(v)^2}$. But then $\delta_1(u) = \delta_2(v)$ for all u, v in $\mathcal{A}^f$ and hence must both be global constants.

□

Proposition 18. *For an integer m and $\sigma = \sigma_g$, for u in $\mathcal{A}^f$, we have*

$$\sigma(mu) = \Phi_{[m],g,g}(u)\sigma(u)^{m^2}.$$

Proof. Let g_n be a local representative for Θ_n in a neighborhood of the origin, defined over R. Define ψ_n to be the division polynomial for multiplication by m on A_n, i.e., $\psi_n = \phi_{[m],g_n \circ [m],g_n}$. Note that $[m]$ is defined over R on $\mathcal{A}$ so $[m]^*g_n$ is defined over R, and recall that the m-torsion form a maximal isotropic subgroup of the m^2-torsion with respect to $m^2\Theta$, so there is a division polynomial. Checking divisors, we have

$$\begin{aligned}(a_n^*\psi_0) &= a_n^*([m]^*\Theta - m^2\Theta)\\ &= [m]^*a_n^*\Theta - m^2a_n^*\Theta\\ &= ([m]^*a_n^*\Theta - [m]^*p^n\Theta_n) - \big(m^2a_n^*\Theta - m^2p^n\Theta_n\big) + \big([m]^*p^n\Theta_n - m^2p^n\Theta_n\big)\\ &= [m]^*\left(a_n^*\Theta - p^n\Theta_n\right) - m^2\left(a_n^*\Theta - p^n\Theta_n\right) + p^n\left([m]^*\Theta_n - m^2\Theta_n\right)\\ &= [m]^*(\phi_n) - m^2(\phi_n) + p^n(\psi_n).\end{aligned}$$

Hence there must be constants c_n such that $c_n \cdot a_n^*\psi_0 = \dfrac{\phi_n \circ [m]}{\phi_n^{m^2}} \cdot \psi_n^{p^n}$. We compute

$$\begin{aligned}c_n \cdot a_n^*\psi_0 &= \frac{\phi_n \circ [m]}{\phi_n^{m^2}} \cdot \psi_n^{p^n}\\ &= \left(\frac{g_n \circ [m]}{g_n^{m^2}}\right)^{p^n} \cdot \frac{\phi_n \circ [m]}{\phi_n^{m^2}} \cdot \psi_n^{p^n} \cdot \left(\frac{g_n^{m^2}}{g_n \circ [m]}\right)^{p^n}\\ &= \frac{\left(g_n^{p^n} \cdot \phi_n\right) \circ [m]}{\left(g_n^{p^n} \cdot \phi_n\right)^{m^2}} \cdot \left(\psi_n \cdot \frac{g_n^{m^2}}{g_n \circ [m]}\right)^{p^n}\\ &= \frac{\sigma_n \circ [m]}{\sigma_n^{m^2}} \cdot \left(\psi_n \cdot \frac{g_n^{m^2}}{g_n \circ [m]}\right)^{p^n}.\end{aligned}$$

Restricting to the kernels of reduction, since $\psi_n \cdot \frac{g_n^{m^2}}{g_n \circ [m]}$ is a unit power series, the right hand side converges to $\frac{\sigma \circ [m]}{\sigma^{m^2}}$. Thus the left hand side must converge, i.e., the $c_n \to c$ for some c. This gives us $c \cdot \psi_0 = \frac{\sigma \circ [m]}{\sigma^{m^2}}$. Note that $\frac{\sigma}{g}(0_A) = 1$, hence

$$c = c \cdot \psi_0 \cdot \frac{g^{m^2}}{g \circ [m]}(0_A) = \frac{\sigma \circ [m]}{\sigma^{m^2}} \cdot \frac{g^{m^2}}{g \circ [m]}(0_A) = 1.$$

□

Furthermore σ is unique with this property.

Proposition 19. *Let f be an element of $\hat{\mathcal{O}}_{\mathcal{A},0}$ such that $f = g \cdot u$ for some unit power series u and $f \circ [p] = \Phi_{[p],g,g} \cdot f^{p^2}$. Then $f = \sigma$.*

Proof. Possibly after some unramified extension S of R, $\mathcal{A}^f \cong \mathbb{G}_m^g$. Let $t_1, \ldots, t_g$ be a choice of local parameters at the origin defined over S which are parameters for $\mathbb{G}_m^g$. We then have

$$[p]^* t_i = (1 + t_i)^p - 1 \equiv t_i^p \,(\mathrm{mod}\, \pi).$$

Define $\beta = \frac{\sigma}{f}$. Assume that $f \neq \sigma$, i.e., that $\beta \neq 1$. Using the notation that for $m = (m_1, \ldots, m_g)$ in $\mathbb{N}^g$, $|m| = m_1 + \cdots + m_g$, β has an expansion $\beta = 1 + \sum_{|m|=d} b_m t_m^m + O(\text{degree } d+1)$ with the b_m in S, for some minimal degree $d > 0$. At the same time $\beta \circ [p] = \beta^{p^2}$.

Looking at the expansion, we see

$$[p]^* \beta \equiv 1 + \sum_{|m|=d} b_m t_m^{p \cdot m} + O(\text{degree } pd + 1) \,(\mathrm{mod}\, \pi).$$

At the same time,

$$\beta^{p^2} \equiv 1 + \sum_{|m|=d} b_m^{p^2} t_m^{p^2 \cdot m} + O(\text{degree } p^2 d + 1) \,(\mathrm{mod}\, \pi).$$

However, the minimal degrees of the two expressions modulo π differ, which is impossible. Therefore $\beta = 1$.

□

More generally, we have the following result.

Proposition 20. *Let $f : A \to A'$ be an isogeny defined over K which is the quotient by a maximal isotropic subgroup of the m-torsion of A. Let Θ' be a symmetric theta divisor in A' such that $f^*\Theta' \sim m \cdot \Theta$, represented locally by a function g' over R. We have*

$$\sigma' \circ f(Q) = \Phi_{f,g,g'}(Q) \cdot \sigma(Q)^m$$

where $\sigma' = \sigma'_{g'}$ is the sigma function on A', and Q is in $\mathcal{A}^f$. Note that $f(Q)$ is in $(\mathcal{A}')^f$, so this makes sense.

Proof. Following the idea in [29] p. 374, we define $\eta = \frac{f^*\sigma'}{\Phi_{f,g,g'}}$. As power series, we find $\eta = g^m \cdot u$ for some unit power series u with constant coefficient 1, defined over R. Similarly, $\frac{g^n \cdot \Phi_{f,g,g'}}{g'}$ is a power series over R with constant term 1. Note also

$$\begin{aligned}
\frac{\eta([p]Q)}{\eta(Q)^{p^2}} &= \frac{\sigma'(f([p]Q))}{\Phi_{f,g,g'}([p]Q)} \cdot \frac{\Phi_{f,g,g'}(Q)^{p^2}}{\sigma'(f(Q))^{p^2}} && \text{definition of } \eta \\
&= \frac{\sigma'([p]f(Q))}{\Phi_{f\circ[p],g,g'}(Q) \cdot \Phi_{[p],g,g}(Q)^{-m}} \cdot \frac{\Phi_{f,g,g'}(Q)^{p^2}}{\sigma'(f(Q))^{p^2}} && \text{Proposition 6, } f \text{ commutes with } [p] \\
&= \frac{\Phi_{[p],g',g'}(f(Q)) \cdot \sigma'(f(Q))^{p^2}}{\Phi_{f\circ[p],g,g'}(Q) \cdot \Phi_{[p],g,g}(Q)^{-m}} \cdot \frac{\Phi_{f,g,g'}(Q)^{p^2}}{\sigma'(f(Q))^{p^2}} && \text{Proposition 18} \\
&= \frac{\Phi_{[p],g',g'}(f(Q)) \cdot \Phi_{f,g,g'}(Q)^{p^2}}{\Phi_{f\circ[p],g,g'}(Q)} \cdot \Phi_{[p],g,g}(Q)^m && \text{rearrangement} \\
&= \frac{\Phi_{[p]\circ f,g,g'}(Q)}{\Phi_{f\circ[p],g,g'}(Q)} \cdot \Phi_{[p],g,g}(Q)^m && \text{Proposition 6} \\
&= \Phi_{[p],g,g}(Q)^m && f \text{ commutes with } [p].
\end{aligned}$$

Define $\alpha(Q) = \frac{\eta(Q)}{\sigma(Q)^{m-1}}$. We see $\alpha = g \cdot u'$ for some power series u' over R with constant term 1. At the same time

$$\begin{aligned}
\alpha([p]Q) &= \frac{\eta([p]Q)}{\sigma([p]Q)^{m-1}} && \text{definition of } \alpha \\
&= \frac{\Phi_{[p],g,g}(Q)^m \cdot \eta(Q)^{p^2}}{\Phi_{[p],g,g}(Q)^{m-1} \cdot \sigma(Q)^{p^2(m-1)}} && \text{above calculation, Proposition 18} \\
&= \Phi_{[p],g,g}(Q) \cdot \left(\frac{\eta(Q)}{\sigma(Q)^{m-1}}\right)^{p^2} && \text{rearrangement} \\
&= \Phi_{[p],g,g}(Q) \cdot \alpha(Q)^{p^2} && \text{definition of } \alpha.
\end{aligned}$$

Thus α meets the hypothesis of f in Proposition 19, so we must have $\sigma = \alpha$. Then we have $\sigma(Q) = \frac{\eta(Q)}{\sigma(Q)^{m-1}}$ or that $\sigma(Q)^m = \frac{\sigma'(f(Q))}{\Phi_{f,g,g'}(Q)}$. □

If D is an invariant derivation on $\mathcal{O}_{\mathcal{A}}$, then it has a unique extension to the stalk $\mathcal{O}_{\mathcal{A},0}$ and hence a unique extension to the completion $\hat{\mathcal{O}}_{\mathcal{A},0}$. Since D is invariant under translation by any point of $\mathcal{A}$, it is certainly invariant under translation by a point of $\mathcal{A}^f$. We also have extensions of D to $\mathcal{O}_{\mathcal{A}\times\mathcal{A}}$ by acting on either the first or second factor. If $f(u,v)$ is an element of $\hat{\mathcal{O}}_{\mathcal{A}\times\mathcal{A},0}$, by $D^u f$ we shall mean the derivation D acting on the first factor, and similarily for $D^v f$.

Proposition 21. *Let D_1, D_2 be invariant derivations on the formal group at the origin on A, then:*

(a) $\frac{D_1(\sigma)}{\sigma}$ *is in* $g^{-1}R[[t_1,\dots,t_g]]$ *and* $D_2(\frac{D_1(\sigma)}{\sigma})$ *is the restriction of a rational function on* A

(b) if K *is characteristic zero and* f *is in* $g^{-1}R[[t_1,\dots,t_g]]$ *that satisfies* $D_2(f) = D_2\left(\frac{D_1(\sigma)}{\sigma}\right) + c$ *for some constant* c *in* R*, then* $f = \frac{D_1(\sigma)}{\sigma}$*.*

Proof.

(a) The expression $h(u,v) = \frac{\sigma(u+v)\sigma(u-v)}{\sigma(u)^2\sigma(v)^2}$ represents a rational function on $A \times A$ so logarithmic derivations of h will also be rational functions on $A \times A$. Let D_i^u denote the differential operator which acts as D_i with respect to the variable u. We first compute

$$\begin{aligned}
&(D_j^u + D_j^v)\log\left(\frac{\sigma(u+v)\sigma(u-v)}{\sigma(u)^2\sigma(v)^2}\right)\\
&\qquad= \frac{(D_j^u + D_j^v)\sigma(u+v)}{\sigma(u+v)} + \frac{(D_j^u + D_j^v)\sigma(u-v)}{\sigma(u-v)} - 2\frac{(D_j^u + D_j^v)\sigma(u)}{\sigma(u)} - 2\frac{(D_j^u + D_j^v)\sigma(v)}{\sigma(v)}\\
&\qquad= \frac{(D_j\sigma)(u+v) + (D_j\sigma)(u+v)}{\sigma(u+v)} + \frac{(D_j\sigma)(u-v) - (D_j\sigma)(u-v)}{\sigma(u-v)}\\
&\qquad\qquad - 2\frac{(D_j\sigma)(u) + 0}{\sigma(u)} - 2\frac{0 + (D_j\sigma)(v)}{\sigma(v)}\\
&\qquad= 2\frac{(D_j\sigma)(u+v)}{\sigma(u+v)} - 2\frac{(D_j\sigma)(u)}{\sigma(u)} - 2\frac{(D_j\sigma)(v)}{\sigma(v)}
\end{aligned}$$

so we get

$$\begin{aligned}
&(D_i^u - D_i^v)(D_j^u + D_j^v)\log\left(\frac{\sigma(u+v)\sigma(u-v)}{\sigma(u)^2\sigma(v)^2}\right)\\
&\qquad = (D_i^u - D_i^v)\left(2\frac{(D_j\sigma)(u+v)}{\sigma(u+v)} - 2\frac{(D_j\sigma)(u)}{\sigma(u)} - 2\frac{(D_j\sigma)(v)}{\sigma(v)}\right)\\
&\qquad = D_i^u\left(2\frac{(D_j\sigma)(u+v)}{\sigma(u+v)} - 2\frac{(D_j\sigma)(u)}{\sigma(u)} - 2\frac{(D_j\sigma)(v)}{\sigma(v)}\right)\\
&\qquad\qquad - D_i^v\left(2\frac{(D_j\sigma)(u+v)}{\sigma(u+v)} - 2\frac{(D_j\sigma)(u)}{\sigma(u)} - 2\frac{(D_j\sigma)(v)}{\sigma(v)}\right)\\
&\qquad = 2\frac{\sigma(u+v)(D_iD_j\sigma)(u+v) - (D_i\sigma)(u+v)(D_j\sigma)(u+v)}{\sigma(u+v)^2}\\
&\qquad\qquad - 2\frac{\sigma(u)(D_iD_j\sigma)(u) - (D_i\sigma)(u)(D_j\sigma)(u)}{\sigma(u)^2} - 0\\
&\qquad\qquad - 2\frac{\sigma(u+v)(D_iD_j\sigma)(u+v) - (D_i\sigma)(u+v)(D_j\sigma)(u+v)}{\sigma(u+v)^2} + 0\\
&\qquad\qquad + 2\frac{\sigma(v)(D_iD_j\sigma)(v) - (D_i\sigma)(v)(D_j\sigma)(v)}{\sigma(v)^2}\\
&\qquad = 2\frac{\sigma(v)(D_iD_j\sigma)(v) - (D_i\sigma)(v)(D_j\sigma)(v)}{\sigma(v)^2} - 2\frac{\sigma(u)(D_iD_j\sigma)(u) - (D_i\sigma)(u)(D_j\sigma)(u)}{\sigma(u)^2}\\
&\qquad = 2D_iD_j\log(\sigma(v)) - 2D_iD_j\log(\sigma(u)).
\end{aligned}$$

Thus we have

$$(D_i^u - D_i^v)\frac{(D_j^u + D_j^v)h(u,v)}{h(u,v)} = (D_i^u - D_i^v)(D_j^u + D_j^v)\log h(u,v) = 2D_i\frac{D_j\sigma(v)}{\sigma(v)} - 2D_i\frac{D_j\sigma(u)}{\sigma(u)}.$$

We see that

$$D_i\frac{D_j\sigma(u)}{\sigma(u)} = D_i\frac{D_j\sigma(v)}{\sigma(v)} - \frac{1}{2}(D_i^u - D_i^v)\frac{(D_j^u + D_j^v)h(u,v)}{h(u,v)}$$

so fixing v, $D_i\frac{D_j\sigma(u)}{\sigma(u)}$ is the restriction of a rational function on $A\times A$ to A, hence it is the restriction of a rational function on A.

(b) For the second part, note that $D_2\left(f - \frac{D_1(\sigma)}{\sigma}\right) = c$. Base change from R to large enough extension S such that the formal group law is isomorphic to $(\mathbb{G}_m^f)^g$ ([31] Lemma 4.27 shows that the maximal unramified extension of R is sufficient). Let $\tilde{t}_1, \ldots, \tilde{t}_g$ be local parameters for this $(\mathbb{G}_m^f)^g$. Let D be any nonzero invariant derivation on $\hat{\mathcal{O}}_{\mathcal{A},0}$. We can choose $g-1$ other derivations $\tilde{D}_2, \ldots, \tilde{D}_g$ to yield a basis of invariant derivations $D, \tilde{D}_2, \ldots, \tilde{D}_g$. There is then a dual basis of

$\omega, \omega_2, \ldots, \omega_g$ of invariant differentials on $\mathcal{A}^f$ given by

$$d\tilde{f} = (D\tilde{f})\omega + (\tilde{D}_2\tilde{f})\omega_2 + \cdots + (\tilde{D}_g\tilde{f})\omega_g.$$

If $Df = c$, then $\int c \cdot \omega$ would have integral coefficients as a power series in $\tilde{t}_1, \ldots, \tilde{t}_g$. On the other hand, over L, the field of fractions of S, $x \mapsto \int_0^x c \cdot \omega$ is a homomorphism of formal group laws over L from $(\mathbb{G}_m^f)^g \to \mathbb{G}_a^f$. If the coefficients were in S, this would extend to a morphism of formal group laws over S. However $(\mathbb{G}_m^f)^g$ is finite height while $\mathbb{G}_a^f$ is not, so no nontrivial such morphism can exist. Thus it must have been that $c = 0$.

□

Remark: in part (b), even taking f in $g^{-1}K[[t_1, \ldots, t_g]]$ and c in K, we get that $f = \frac{D_1(\sigma)}{\sigma}$ because otherwise after multiplying by a high enough power of π, we would have some Laurent series $\tilde{f}$ with coefficients in R and $D\tilde{f}$ a nonzero constant in R, which is impossible.

Chapter 3

Weierstrass zeta functions on curves of genus two

3.1 Preliminaries on curves

A curve X over a field k is a one dimensional variety (recall our definition of variety at the beginning of Chapter 2). Most of the curves we will be interested in will be smooth.

To any curve X over an algebraically closed field F, we have the group $\mathrm{Div}(X)$ of divisors on X. By definition, $\mathrm{Div}(X)$ is the group of formal finite $\mathbb{Z}$-linear sums of points on X. There is a group homomorphism, called the degree map, $\deg : \mathrm{Div}(X) \to \mathbb{Z}$ defined by taking an element $\sum n_P P$ to the sum of the coefficients $\sum n_P$ (note that all but finitely many n_p are zero). The kernel of the degree map is denoted $\mathrm{Div}^0(X)$. Any nonzero meromorphic function f on X has an associated divisor $(f) = \sum n_P P$ where the n_P is the order of vanishing of f at the point P (positive if f vanishes at P, negative if f has a pole at P, zero otherwise). Such a divisor is said to be a principal divisor.

In the case that X is smooth and projective, all principal divisors have degree zero, and thus form a subgroup of $\mathrm{Div}^0(X)$. Two divisors D_1 and D_2 which differ by a principal divisor are said to be linearly equivalent which we denote by $D_1 \sim D_2$. A divisor is said to be effective if it is a nonnegative sum of points. Define $\mathcal{L}(D)$ to be the set of all meromorphic functions f such that $(f) + D$ is effective (along with 0) which naturally has the structure of a vector space over F. One proves $\mathcal{L}(D)$ is finite dimensional, and its dimension is denoted $\ell(D)$.

A fundamental result in the theory of curves is the Riemann–Roch theorem, which states that for any divisor D on a smooth projective curve X of genus g,

$$\ell(D) - \ell(K - D) = \deg(D) - g + 1$$

where K is a divisor which records the orders of vanishing of a holomorphic differential on X (since any holomorphic differentials differ by multiplication by a function f, different choices will be linearly equivalent), also called a canonical divisor of X.

3.1.1 Hyperelliptic curves

A smooth projective curve X of genus g at least two is said to be hyperelliptic if it admits a morphism of degree 2 to $\mathbb{P}^1_k$. The curve then has an involution ι, called the hyperelliptic involution, which exhanges the points in each fiber of this map. See [44] for a treatment of the theory over the complex numbers.

Over an algebraically closed field $\overline{k}$, X can be covered by two affine patches of the form

$$y^2 = f(x) = x^{2g+1} + \sum_{i=1}^{2g+1} a_i x^{2g+1-i}$$

and

$$y'^2 = x' + \sum_{i=1}^{2g+1} a_i x^{i+1}$$

where $f(x)$ has no repeated roots, $x' = \frac{1}{x}$, $y' = \frac{y}{x^{g+1}}$ and the a_i are in $\overline{k}$. Note that the solution of the second equation has a single point not on the first, given by $x' = y' = 0$. This point will be called ∞. Along with the solutions to $y = 0$, these are the $2g + 2$ Weierstrass points on X.

If the a_i are in k (for k not necessarily algebraically closed), then these affine charts still yield a smooth projective curve of genus two. In this case, X has at least one point defined over k, as ∞ is k-rational.

In this chapter, we will be interested in smooth projective curves of genus two, which are always hyperelliptic. In this case, the canonical divisor has degree two, being given by any pair of conjugate points under ι (or the same point twice for points fixed under ι). Many of the calculations in this chapter, especially most involving expansions of functions in terms of local parameters, were computed or checked using Mathematica.

3.2 Weierstrass zeta functions in genus two

Let b_1, b_2, b_3, b_4, b_5 be independent indeterminants. We will work as generally as possible and consider the curve X of genus 2 given by

$$y^2 = x^5 + b_1x^4 + b_2x^3 + b_3x^2 + b_4x + b_5$$

over $\mathbb{Q}(b_1, \ldots, b_5)$. Note that as a polynomial in $b_1, \ldots, b_5$, the discriminant is not zero, so X is indeed smooth of genus two. We will eventually want to work over the ring $\hat{R}$ which is the completion of $\mathbb{Z}[b_1, \ldots, b_5][H_1^{-1}]$ with respect to the ideal generated by p, where H_1 is the determinant of the Hasse-Witt matrix attached to the curve. We will fix $p \neq 2$ a prime integer.

The functions x and y are regular away from ∞. They have poles of order 2 and 5, respectively, at ∞. For convenience, define $t = -\frac{x^2}{y}$. As x and y have poles of order 2 and 5 at ∞, we see t is a local parameter (vanishes to order 1) at ∞.

Seeing that $y^2 = x^5 + b_1x^4 + b_2x^3 + b_3x^2 + b_4x + b_5$, we have

$$\frac{1}{x} = t^2 + b_1t^2\frac{1}{x} + b_2t^2\left(\frac{1}{x}\right)^2 + b_3t^2\left(\frac{1}{x}\right)^3 + b_4t^2\left(\frac{1}{x}\right)^4 + b_5t^2\left(\frac{1}{x}\right)^5.$$

By repeatedly substituting this formula in for $\frac{1}{x}$ we get an infinite expansion of $\frac{1}{x}$ in terms of t

$$\frac{1}{x} = t^2 + b_1t^4 + \left(b_1^2 + b_2\right)t^6 + \left(b_1^3 + 3b_1b_2 + b_3\right)t^8 + \left(b_1^4 + 6b_1^2b_2 + 4b_1b_3 + 2b_2^2 + b_4\right)t^{10} + O(t^{12}) \quad (3.1)$$

with coefficients in $\mathbb{Z}[b_1 \ldots, b_5]$, where $O(t^a)$ means a power series in t whose coefficients for monomials of degree strictly less than a are all zero. We can invert this formula and get a t-expansion for x

$$x = \frac{1}{t^2} - b_1 - b_2t^2 - (b_1b_2 + b_3)t^4 - \left(b_1^2b_2 + 2b_1b_3 + b_2^2 + b_4\right)t^6 + O(t^8) \quad (3.2)$$

whose coefficients are still in $\mathbb{Z}[b_1 \ldots, b_5]$. Noting that $y = -tx^3 - b_1tx^2 - b_2tx - b_3t - b_4t\frac{1}{x} - b_5t\left(\frac{1}{x}\right)^2$ we get expansions

$$y = -\frac{1}{t^5} + \frac{2b_1}{t^3} + \frac{2b_2 - b_1^2}{t} + 2b_3t + \left(b_2^2 + 2b_1b_3 + 2b_4\right)t^3 + O\left(t^5\right) \quad (3.3)$$

and

$$\begin{aligned}\frac{1}{y} = -t^5 - 2b_1t^7 - \left(3b_1^2 + 2b_2\right)t^9 - \left(4b_1^3 + 8b_1b_2 + 2b_3\right)t^{11} \\ - \left(5b_1^4 + 5b_2^2 + 20b_1^2b_2 + 10b_1b_3 + 2b_4\right)t^{13} + O\left(t^{15}\right).\end{aligned} \tag{3.4}$$

In particular, all of these expansions are produced entirely by adding and multiplying elements with coefficients in $\mathbb{Z}[b_1, \ldots, b_5]$.

The curve X has a standard basis of holomorphic differentials $\omega_1 = \frac{dx}{2y}$ and $\omega_2 = \frac{xdx}{2y}$. Using the above expansions, we compute

$$\begin{aligned}\frac{dx}{2y} = \Big(t^2 + 2b_1t^4 + 3\left(b_1^2 + b_2\right)t^6 + 4\left(b_1^3 + 3b_1b_2 + b_3\right)t^8 \\ + 5\left(b_1^4 + 2b_2^2 + 6b_1^2b_2 + 4b_1b_3 + b_4\right)t^{10} + O\left(t^{12}\right)\Big)dt\end{aligned} \tag{3.5}$$

and

$$\begin{aligned}\frac{xdx}{2y} = \Big(1 + b_1t^2 + \left(b_1^2 + 2b_2\right)t^4 + \left(b_1^3 + 6b_1b_2 + 3b_3\right)t^6 \\ + \left(b_1^4 + 6b_2^2 + 12b_1^2b_2 + 12b_1b_3 + 4b_4\right)t^8 + O\left(t^{10}\right)\Big)dt.\end{aligned} \tag{3.6}$$

By the Riemann-Roch Theorem, both differentials must vanish twice—ω_1 vanishes to order 2 at ∞ while ω_2 vanishes at the two solutions to $x = 0$.

3.2.1 Hasse-Witt matrices

We will start by producing functions with prescribed shape.

Proposition 22. *For each positive integer $k \neq 1, 3$, there exists an unique function on X, regular away from ∞, with t expansions*

$$\rho_k = \frac{1}{t^k} + \frac{M_k}{t^3} + \frac{N_k}{t} + O(t)$$

for some elements M_k, N_k in $\mathbb{Z}[b_1, \ldots, b_5]$.

Proof. The point ∞ is a Weierstrass point of X, so over $\mathbb{Q}(b_1, \ldots, b_5)$, Riemann-Roch tells us that $\ell(\infty) = 1$, $\ell(2 \cdot \infty) = 2$, $\ell(3 \cdot \infty) = 2$, $\ell(4 \cdot \infty) = 3$, and $\ell(n \cdot \infty) = n - 1$ for $n > 4$. This means for each $m \neq 1, 3$, there is a one dimensional coset space of functions (over $\mathbb{Q}(b_1, \ldots, b_5)$)

$$\mathcal{L}(m \cdot \infty)/\mathcal{L}((m-1) \cdot \infty).$$

If we further require that the lead coefficients of the t-expansion are 1, we get a unique coset (for each m) given by all functions with t-expansions of the form $\frac{1}{t^m} + O(t^{1-m})$.

We can do better and specify explicit elements in each of these cosets. Take $\tilde{\rho}_2 = x$ and $\tilde{\rho}_5 = -y$ as representatives when m is 2 or 5. Since every positive integer not 1 or 3 can be written as a positive integer combination of 2 and 5, we can take representatives $\tilde{\rho}_m$ as products $x^i(-y)^j$, where $2i + 5j = m$. At the same time, as x and y are Laurent series in t with coefficients in $\mathbb{Z}[b_1, \ldots, b_5]$ so also are all of the $\tilde{\rho}_m$. There are unique $\mathbb{Q}(b_1, \ldots, b_5)$-linear combinations of the $\tilde{\rho}_m$ which give ρ_k. As the lead coefficients of each $\tilde{\rho}_m$ are 1 and all other coefficients are in $\mathbb{Z}[b_1, \ldots, b_5]$, these linear combinations have coefficients in $\mathbb{Z}[b_1, \ldots, b_5]$. □

For each positive integer n, we will define

$$\phi_n = \rho_{3p^n} = \frac{1}{t^{3p^n}} + \frac{A_n}{t^3} + \frac{B_n}{t} + O(1)$$

$$\psi_n = \rho_{p^n} = \frac{1}{t^{p^n}} + \frac{C_n}{t^3} + \frac{D_n}{t} + O(1)$$

for some elements A_n, B_n, C_n, D_n in $\mathbb{Z}[b_1, \ldots, b_5]$.

We see that $-\iota^*\phi_n = \frac{1}{t^{3p^n}} + \frac{A_n}{t^3} + \frac{B_n}{t} + O(1)$ since $t \mapsto -t$ under ι. The uniqueness of ρ_k implies $\iota^*\phi_n = -\phi_n$. Similarly, $\iota^*\psi_n = -\psi_n$. As t is odd, only odd powers of t can show up in the t-expansions of the ϕ_n and ψ_n.

In particular, there are elements $A_n, B_n, C_n, D_n, I_n, J_n, R_n, S_n$ in $\mathbb{Z}[b_1, \ldots, b_5]$ such that

$$\phi_n = \frac{1}{t^{3p^n}} + \frac{A_n}{t^3} + \frac{B_n}{t} + I_n t + R_n t^3 + O(t^5)$$

and

$$\psi_n = \frac{1}{t^{p^n}} + \frac{C_n}{t^3} + \frac{D_n}{t} + J_n t + S_n t^3 + O(t^5).$$

There is an inductive relation on these coefficients modulo p.

Proposition 23. *For each $n \geq 1$*

$$\begin{bmatrix} A_{n+1} & B_{n+1} & I_{n+1} & R_{n+1} \\ C_{n+1} & D_{n+1} & J_{n+1} & S_{n+1} \end{bmatrix} \equiv - \begin{bmatrix} A_n^p & B_n^p \\ C_n^p & D_n^p \end{bmatrix} \begin{bmatrix} A_n & B_n & I_n & R_n \\ C_n & D_n & J_n & S_n \end{bmatrix} \pmod{p}$$

Proof. Note first that by taking all of the coefficients defining X modulo p, we get a smooth curve X_p over $\mathbb{F}_p(b_1,\dots,b_5)$ which is also of genus 2 (the discriminant of $x^5+b_1x^4+b_2x^3+b_3x^2+b_4x+b_5$ does not vanish identically modulo p). Then consider the mod p t-expansions of the functions

$$\begin{aligned}\phi_n^p-\phi_{n+1}-A_n^p\phi_1-B_n^p\psi_1 \equiv&(-A_{n+1}-A_n^pA_1-B_n^pC_1)t^{-3}+(-B_{n+1}-A_n^pB_1-B_n^pD_1)t^{-1}\\&+(-I_{n+1}-A_n^pI_1-B_n^pJ_1)t+(-R_{n+1}-A_n^pR_1-B_n^pS_1)t^3+\cdots\end{aligned}$$

and

$$\begin{aligned}\psi_n^p-\psi_{n+1}-C_n^p\phi_1-D_n^p\psi_1 \equiv&(-C_{n+1}-C_n^pA_1-D_n^pC_1)t^{-3}+(-D_{n+1}-C_n^pB_1-D_n^pD_1)t^{-1}\\&+(-J_{n+1}-C_n^pI_1-D_n^pJ_1)t+(-S_{n+1}-C_n^pR_1-D_nS_1)t^3+\cdots.\end{aligned}$$

Both functions are regular away from ∞ so, over $\mathbb{F}_p(b_1,\dots,b_5)$, the coefficients of t^{-3} must vanish since $\ell(3\infty)=\ell(2\infty)$. But then similarly the coefficients of t^{-1} must vanish and both functions are constant (hence 0) and all coefficients vanish (mod p). This gives

$$\begin{aligned}-A_{n+1}&\equiv A_n^pA_1+B_n^pC_1 & -B_{n+1}&\equiv A_n^pB_1+B_n^pD_1\\ -C_{n+1}&\equiv C_n^pA_1+D_n^pC_1 & -D_{n+1}&\equiv C_n^pB_1+D_n^pD_1\\ -I_{n+1}&\equiv A_n^pI_1+B_n^pJ_1 & -R_{n+1}&\equiv A_n^pR_1+B_n^pS_1\\ -J_{n+1}&\equiv C_n^pI_1+D_n^pJ_1 & -S_{n+1}&\equiv C_n^pR_1+D_n^pS_1.\end{aligned}$$

□

This computation yields an explicit expression for the determinants of the A_n, B_n, C_n, D_n and ultimately an invertibility criterion.

Corollary 24. *For each $n\ge 0$, there is a congruence*

$$\begin{vmatrix}A_{n+1} & B_{n+1}\\ C_{n+1} & D_{n+1}\end{vmatrix} \equiv \begin{vmatrix}A_1 & B_1\\ C_1 & D_1\end{vmatrix}^{p^n+p^{n-1}+\cdots+p+1} \pmod p.$$

Proof. Induct on n. The result clearly holds for $n=0$. Taking determinants of the first two columns from Proposition 23 we have

$$\begin{vmatrix} A_{n+1} & B_{n+1} \\ C_{n+1} & D_{n+1} \end{vmatrix} \equiv \begin{vmatrix} A_n^p & B_n^p \\ C_n^p & D_n^p \end{vmatrix} \begin{vmatrix} A_1 & B_1 \\ C_1 & D_1 \end{vmatrix} \equiv \begin{vmatrix} A_n & B_n \\ C_n & D_n \end{vmatrix}^p \begin{vmatrix} A_1 & B_1 \\ C_1 & D_1 \end{vmatrix} \pmod{p}$$

hence if the result is true for n, we have

$$\begin{vmatrix} A_{n+1} & B_{n+1} \\ C_{n+1} & D_{n+1} \end{vmatrix} \equiv \left(\begin{vmatrix} A_1 & B_1 \\ C_1 & D_1 \end{vmatrix}^{p^{n-1}+\cdots+p+1} \right)^p \begin{vmatrix} A_1 & B_1 \\ C_1 & D_1 \end{vmatrix} \pmod{p}.$$

□

Let $H_n = A_nD_n - B_nC_n$. We will invert H_1 in our coefficient ring, thus considering only curves with H_1 invertible. By the corollary, we have $H_n \equiv H_1^{\frac{p^n-1}{p-1}} \pmod{p}$. There is the following invertibility lemma.

Lemma 25. *Let R be a ring in which the rational prime p is not invertible. If u in R is invertible modulo p, then u is invertible modulo p^m for any $m \geq 1$. In particular, u is invertible in $\varprojlim R/p^mR$.*

Proof. Proceed by induction. If u is invertible modulo p^m, $m \geq 1$, then there exist v and q in R such that $uv + p^mq = 1$. Raising to the pth power, we get

$$1 = (uv + p^mq)^p = \sum_{i=0}^{p} \binom{p}{i} p^{im} q^i u^{p-i} v^{p-i} = u^p v^p + p^{m+1} Q$$

for some Q in R, and hence $u \cdot u^{p-1}v^p \equiv 1 \pmod{p^{m+1}}$. □

Define the ring $\hat{R}$ as the completion of $\mathbb{Z}[b_1, \ldots, b_5][H_1^{-1}]$ with respect to the ideal generated by p. Applying Corollary 24 and Lemma 25 we see that H_n is invertible in $\mathbb{Z}[b_1, \ldots, b_5][H_1^{-1}]/(p^{m+1})$ for every positive m, which is to say that H_n is invertible in $\hat{R}$ for every n.

3.2.2 Weierstrass zeta functions

The zeta functions we will produce are Laurent series whose t expansions will be of the form $\frac{1}{t^3} + O(t)$ and $\frac{1}{t} + O(t)$. Riemann-Roch definitively says no such rational functions on X without poles away from ∞ exist, so instead they will be functions on some "formal neighborhood" of ∞

(i.e., they will be convergent series for any points which reduce modulo p to ∞ with the exception of ∞ itself). They will be produced as p-adic limits of t expansions of actual meromorphic functions on X.

Since H_n is invertible $\hat{R}$, we can define functions $\zeta_{1,n}$ and $\zeta_{2,n}$ by

$$\begin{bmatrix} \zeta_{1,n} \\ \zeta_{2,n} \end{bmatrix} = \begin{bmatrix} A_n & B_n \\ C_n & D_n \end{bmatrix}^{-1} \begin{bmatrix} \phi_n \\ \psi_n \end{bmatrix} = \frac{1}{A_nD_n - B_nC_n} \begin{bmatrix} D_n & -B_n \\ -C_n & A_n \end{bmatrix} \begin{bmatrix} \phi_n \\ \psi_n \end{bmatrix}.$$

If we define the constants $\alpha_n, \beta_n, \gamma_n, \delta_n$ by

$$\begin{bmatrix} \alpha_n & \delta_n \\ \beta_n & \gamma_n \end{bmatrix} = \begin{bmatrix} A_n & B_n \\ C_n & D_n \end{bmatrix}^{-1} \begin{bmatrix} I_n & R_n \\ J_n & S_n \end{bmatrix} = \frac{1}{A_nD_n - B_nC_n} \begin{bmatrix} D_n & -B_n \\ -C_n & A_n \end{bmatrix} \begin{bmatrix} I_n & R_n \\ J_n & S_n \end{bmatrix}$$

we get t expansions

$$\begin{aligned} \zeta_{1,n} &= \frac{D_n}{H_n} t^{-3p^n} + \frac{-B_n}{H_n} t^{-p^n} + \frac{1}{t^3} + \alpha_n t + \delta_n t^3 + O(t^5) \\ \zeta_{2,n} &= \frac{-C_n}{H_n} t^{-3p^n} + \frac{A_n}{H_n} t^{-p^n} + \frac{1}{t} + \beta_n t + \gamma_n t^3 + O(t^5). \end{aligned}$$

Note that these have been chosen exactly so that after application of any derivation of function fields, the lead terms will vanish modulo p^n. Let $\omega_1 = \frac{dx}{2y}$. This is a regular differential form which vanishes to order 2 at ∞ and nowhere else, so the derivatives $\frac{d\zeta_{1.n}}{\omega_1}$ and $\frac{d\zeta_{2,n}}{\omega_1}$ are meromorphic functions on X with poles at ∞ of order $3p^n + 1$ and $p^n + 1$, respectively, and nowhere else. Inverting Equation (3.5) we have

$$\frac{dt}{\omega_1} = \frac{1}{t^2} - 2b_1 - (3b_2 - b_1^2)t^2 - 4b_3t^4 - (b_2^2 + 4b_1b_3 + 5b_4)t^6 + O(t^8) \tag{3.7}$$

so looking at t expansions modulo p^n, we have

$$\begin{aligned} -\frac{d\zeta_{1,n}}{\omega_1} &\equiv -\left(\frac{d\zeta_{1,n}}{dt} + 3p^n \frac{D_n}{H_n} \rho_{3p^n+1} - p^n \frac{B_n}{H_n} \rho_{p^n+1} \right) \frac{dt}{\omega_1} \\ &= 3x^3 + 3b_1x^2 - \alpha_n x - (3b_1b_2 - b_1\alpha_n + 3b_3 + 3\delta_n) \pmod{p^n} \end{aligned} \tag{3.8}$$

and

$$\begin{aligned} -\frac{d\zeta_{2,n}}{\omega_1} &\equiv -\left(\frac{d\zeta_{2,n}}{dt} - 3p^n \frac{C_n}{H_n} \rho_{3p^n+1} + p^n \frac{A_n}{H_n} \rho_{p^n+1} \right) \frac{dt}{\omega_1} \\ &= x^2 - \beta_n x - (b_2 - b_1\beta_n + 3\gamma_n) \pmod{p^n}. \end{aligned} \tag{3.9}$$

Note that the middle expressions in Equations 3.8 and 3.9 are meromorphic functions regular away from ∞ and have a pole at ∞ of order 6 and 4 respectively, and hence must be cubic and quadratic polynomials in x over $\mathbb{Q}(b_1, \ldots, b_5)$. We will see that these polynomials in x are unique modulo p^n.

Lemma 26. *If $\xi = \sum_{i=-m}^{\infty} \xi_i t^i$ is any Laurent series in t with coefficients in $\hat{R}$ such that $\frac{d\xi}{\omega_1} \equiv rx + s \pmod{p^n}$ for any r and s in $\hat{R}$, then $r \equiv s \equiv 0 \pmod{p^n}$.*

Proof. As $\frac{d\xi}{\omega_1} = \frac{d\xi}{dt} \cdot \frac{dt}{\omega_1} \equiv rx + s \pmod{p^n}$, we will define $\eta = (rx+s)\omega_1$. Then η is a holomorphic differential on X with t expansion $\eta = \sum_{i=0}^{\infty} \eta_i t^i dt = (r + (rb_1 + s)t^2 + O(t^4))dt$.

We see that $\phi_n \eta$ and $\psi_n \eta$ are meromorphic differentials with poles only at ∞. Since these have only a single pole, the corresponding residue must be zero. At the same time, the residues of these differentials are given by the coefficient of $\frac{dt}{t}$ in their t-expansions. We have

$$\phi_n \eta = \left(\frac{1}{t^{3p^n}} + \frac{A_n}{t^3} + \frac{B_n}{t} + I_n t + R_n t^3 + O(t^5) \right) \sum_{i=0}^{\infty} \eta_i t^i dt$$

and

$$\psi_n \eta = \left(\frac{1}{t^{p^n}} + \frac{C_n}{t^3} + \frac{D_n}{t} + J_n t + S_n t^3 + O(t^5) \right) \sum_{i=0}^{\infty} \eta_i t^i dt$$

so we get

$$0 = \operatorname{Res}_{\infty} \phi_n \eta = \eta_{3p^n-1} + A_n \eta_2 + B_n \eta_0 = \eta_{3p^n-1} + (rb_1 + s)A_n + rB_n$$

and

$$0 = \operatorname{Res}_{\infty} \psi_n \eta = \eta_{p^n-1} + C_n \eta_2 + D_n \eta_0 = \eta_{p^n-1} + (rb_1 + s)C_n + rD_n.$$

Since $d\xi \equiv \eta \pmod{p^n}$, we have $\frac{d\xi}{dt} \equiv \frac{\eta}{dt} \pmod{p^n}$. In particular $\eta_{3p^n-1} \equiv 3p^n \xi_{3p^n} \equiv 0 \pmod{p^n}$ and similarly $\eta_{p^n-1} \equiv p^n \xi_{p^n} \equiv 0 \pmod{p^n}$. The residue equations then force

$$\begin{bmatrix} A_n & B_n \\ C_n & D_n \end{bmatrix} \begin{bmatrix} \eta_2 \\ \eta_0 \end{bmatrix} \equiv \begin{bmatrix} A_n & B_n \\ C_n & D_n \end{bmatrix} \begin{bmatrix} rb_1 + s \\ r \end{bmatrix} \equiv \begin{bmatrix} 0 \\ 0 \end{bmatrix} \pmod{p^n}.$$

At the end of the Section 3.2.1, we found that $H_n = A_n D_n - B_n C_n$ is invertible in $\hat{R}$, and so follows the lemma. □

We get the promised uniqueness.

Proposition 27. *The polynomial $x^2 - \beta_n x - (b_2 - b_1\beta_n + 3\gamma_n)$ is the unique $(\operatorname{mod} p^n)$ monic quadratic polynomial $f(x)$ such that there exists ξ_2, a Laurent series in t with coefficients in $\hat{R}$, such that $\frac{d\xi}{\omega_1} \equiv f(x) \pmod{p^n}$. The polynomial $3x^3 + 3b_1x^2 - \alpha_n x - (3b_1b_2 - b_1\alpha_n + 3b_3 + 3\delta_n)$ is the unique $(\operatorname{mod} p^n)$ cubic polynomial $g(x)$ with lead coefficient 3 and quadratic coefficient $3b_1$ such that there exists ξ_1, a Laurent series in t with coefficients in $\hat{R}$, such that $\frac{d\eta}{\omega_1} \equiv g(x) \pmod{p^n}$.*

Proof. Note that $-\zeta_{2,n}$ can be taken as ξ_2. The polynomial $f(x)$ is unique by Lemma 26. Similarly, $-\zeta_{1,n}$ can be taken to be ξ_1 and $g(x)$ is unique by the lemma. □

We will now see that this uniqueness forces the sequence of polynomials $3x^3 + 3b_1x^2 - \alpha_n x - (3b_1b_2 - b_1\alpha_n + 3b_3 + 3\delta_n)$ and $x^2 - \beta_n x - (b_2 - b_1\beta_n + 3\gamma_n)$ to converge as polynomials over $\hat{R}$.

Corollary 28. *For each $n \geq 1$ there are congruences of polynomials*

$$3x^3+3b_1x^2-\alpha_{n+1}x-(3b_1b_2-b_1\alpha_{n+1}+3b_3+3\delta_{n+1}) \equiv 3x^3+3b_1x^2-\alpha_n x-(3b_1b_2-b_1\alpha_n+3b_3+3\delta_n) \pmod{p^n}$$

$$x^2 - \beta_{n+1}x - (b_2 - b_1\beta_{n+1} + 3\gamma_{n+1}) \equiv x^2 - \beta_n x - (b_2 - b_1\beta_n + 3\gamma_n) \pmod{p^n}$$

or equivalently, there are congruences $\alpha_{n+1} \equiv \alpha_n$, $\beta_{n+1} \equiv \beta_n$, $\delta_{n+1} \equiv \delta_n$, $\gamma_{n+1} \equiv \gamma_n$ modulo p^n (if $p = 3$, the coefficients are congruent modulo 3^{n-1}).

Proof. Since $3x^3+3b_1x^2-\alpha_{n+1}x-(3b_1b_2-b_1\alpha_{n+1}+3b_3+3\delta_{n+1})$ satisfies the condition of Proposition 28 modulo p^{n+1}, it also satisfies the condition modulo p^n. At the same time $3x^3 + 3b_1x^2 - \alpha_n x - (3b_1b_2-b_1\alpha_n+3b_3+3\delta_n)$ satisfies the condition modulo p^n. The uniqueness of the proposition implies they must be congruent modulo p^n. The same argument works for $x^2-\beta_{n+1}x-(b_2-b_1\beta_{n+1}+3\gamma_{n+1})$. □

In particular, as elements of $\hat{R}$, we have convergence $\alpha_n \to \alpha$, $\beta_n \to \beta$, $\delta_n \to \delta$, and $\gamma_n \to \gamma$ for some $\alpha, \beta, \delta, \gamma$. The uniqueness in Proposition 28 also forces convergence of the $\zeta_{1,n}$ and the $\zeta_{2,n}$.

Corollary 29. *Coefficient by coefficient, the sequences $\zeta_{1,n}$ and $\zeta_{2,n}$ converge $\zeta_{1,n} \to \zeta_1$ and $\zeta_{2,n} \to \zeta_2$ for some Laurent series ζ_1 in $\frac{1}{t^3} + \hat{R}[[t]]$ and ζ_2 in $\frac{1}{t} + \hat{R}[[t]]$.*

Proof. Let $i \in \{1,2\}$. Since $\frac{d\zeta_{i,n}}{\omega_1} = \frac{d\zeta_{i,n}}{dt}\frac{dt}{\omega_1}$ and $\frac{d\zeta_{i,n+1}}{\omega_1} \equiv \frac{d\zeta_{i,n}}{\omega_1} \pmod{p^n}$, it must be that $\frac{d\zeta_{i,n+1}}{dt} \equiv \frac{d\zeta_{i,n}}{dt} \pmod{p^n}$. If $\zeta_{i,n} = \sum_k \zeta^{(k)}_{i,n} t^k$, for a fixed k, then we have $\frac{d\zeta^{(k)}_{i,n} t^k}{dt} \equiv \frac{d\zeta^{(k)}_{i,n+1} t^k}{dt} \pmod{p^n}$ and so $k\zeta^{(k)}_{i,n+1} \equiv k\zeta^{(k)}_{i,n+1} \pmod{p^n}$. For $n > \nu_p(k)$ (where $\nu_p(k)$ is the number of times p divides the integer k), we have $\zeta^{(k)}_{i,n} \equiv \zeta^{(k)}_{i,n+1} \pmod{p^{n-\nu_p(k)}}$ and hence there is convergence $\zeta^{(k)}_{i,n} \to \zeta^{(k)}_i$ for each k. □

By construction, we have

$$-\frac{d\zeta_1}{\omega_1} = 3x^3 + 3b_1x^2 - \alpha x - (3b_1b_2 - b_1\alpha + 3b_3 + 3\delta)$$

and

$$-\frac{d\zeta_2}{\omega_1} = x^2 - \beta x - (b_2 - b_1\beta + 3\gamma).$$

Remark: The vector space H^1_{dR} is generated by $\omega_1 = \frac{dx}{2y}$, $\omega_2 = \frac{xdx}{2y}$, $\frac{x^2dx}{2y}$, and $\frac{x^3dx}{2y}$, with the first two generating the space of holomorphic differentials on X. We see that $d\zeta_1 = (3x^3 + 3b_1x^2 - \alpha x - (3b_1b_2 - b_1\alpha + 3b_3 + 3\delta))\omega_1$ and $d\zeta_2 = (x^2 - \beta x - (b_2 - b_1\beta + 3\gamma))\omega_1$ generate the two dimensional subspace of $H^1_{dR}(X)$ which is comprised of exactly those meromorphic differentials in $H^1_{dR}(X)$ which integrate to give Laurent series whose coefficients have bounded powers of p.

3.2.3 Universal p-adic zeta functions

If K is a field of characteristic zero, complete with respect to a nonarchimedean absolute value $|\cdot|_\nu$, with ring of integers R and maximal ideal containing p (in particular complete with respect to the p-adic topology), and if

$$y^2 = x^5 + a_1x^4 + a_2x^3 + a_3x^2 + a_4x + a_5$$

is the affine model of a smooth genus two curve with coefficients in R and $|H_1(a_1,\dots,a_5)|_\nu = 1$, there is a ring homomorphism $\mathbb{Z}[b_1,\dots,b_5][\frac{1}{H_1}] \to R$ taking $b_i \mapsto a_i$. This homomorphism extends to all of $\hat{R}$ by continuity, since R is p-complete. The induced base change on X yields the curve above. Since X was defined over $\hat{R}$ as are all of the coefficients of ζ_1, ζ_2, the base change to R produces Laurent series $\zeta_{1,R}$ and $\zeta_{2,R}$ with coefficients in R which exhibit all of the properties of

ζ_1 and ζ_2 (it is essential that R be complete, as the coefficients of the ζ_i are limits of the b_i, hence the coefficients of the $\zeta_{i,R}$ are limits of the a_i).

In this way, for any genus two curve C over K with a rational Weierstrass point and invertible Hasse-Witt matrix, by expressing C with an affine model $y^2 = x^5 + a_1x^4 + a_2x^3 + a_3x^2 + a_4x + a_5$ where $|a_i|_\nu \leq 1$, we get a pair of Weierstrass zeta functions ζ_1 and ζ_2, which are Laurent series in t with coefficients in R.

3.2.4 Appendix: t-expansions

For a genus two curve with the following affine equation

$$y^2 = x^5 + b_1x^4 + b_2x^3 + b_3x^2 + b_4x + b_5$$

with local parameter at ∞

$$t = -\frac{x^2}{y}$$

we get:

$$
\begin{aligned}
x &= \frac{1}{t^2} - b_1 - b_2 t^2 - (b_1 b_2 + b_3) t^4 - \left(b_1^2 b_2 + 2 b_1 b_3 + b_2^2 + b_4\right) t^6 \\
&\qquad\qquad - \left(b_1^3 b_2 + 3 b_1^2 b_3 + 3 b_1 b_2^2 + 3 b_1 b_4 + 3 b_2 b_3 + b_5\right) t^8 + O(t^{10}) \\
y &= -\frac{1}{t^5} + \frac{2 b_1}{t^3} + \frac{2 b_2 - b_1^2}{t} + 2 b_3 t + \left(b_2^2 + 2 b_1 b_3 + 2 b_4\right) t^3 \\
&\qquad\qquad + 2 \left(b_3 b_1^2 + b_1 b_2^2 + 2 b_1 b_4 + 2 b_2 b_3 + b_5\right) t^5 + O\left(t^7\right) \\
\frac{1}{x} &= t^2 + b_1 t^4 + \left(b_1^2 + b_2\right) t^6 + \left(b_1^3 + 3 b_1 b_2 + b_3\right) t^8 + \left(b_1^4 + 6 b_1^2 b_2 + 4 b_1 b_3 + 2 b_2^2 + b_4\right) t^{10} \\
&\qquad\qquad + \left(b_1^5 + 10 b_1^3 b_2 + 10 b_1^2 b_3 + 10 b_1 b_2^2 + 5 b_1 b_4 + 5 b_2 b_3 + b_5\right) t^{12} + O(t^{14}) \\
\frac{1}{y} &= -t^5 - 2 b_1 t^7 - \left(3 b_1^2 + 2 b_2\right) t^9 - \left(4 b_1^3 + 8 b_1 b_2 + 2 b_3\right) t^{11} - \left(5 b_1^4 + 5 b_2^2 + 20 b_1^2 b_2 + 10 b_1 b_3 + 2 b_4\right) t^{13} \\
&\qquad\qquad - \left(6 b_1^5 + 30 b_1 b_2^2 + 40 b_1^3 b_2 + 30 b_1^2 b_3 + 12 b_2 b_3 + 12 b_1 b_4 + 2 b_5\right) t^{15} + O\left(t^{17}\right) \\
\frac{\omega_1}{dt} &= t^2 + 2 b_1 t^4 + 3 \left(b_1^2 + b_2\right) t^6 + 4 \left(b_1^3 + 3 b_1 b_2 + b_3\right) t^8 + 5 \left(b_1^4 + 2 b_2^2 + 6 b_1^2 b_2 + 4 b_1 b_3 + b_4\right) t^{10} \\
&\qquad\qquad + 6 \left(b_1^5 + 10 b_1^3 b_2 + 10 b_1^2 b_3 + 5 b_2 b_3 + 10 b_1 b_2^2 + 5 b_1 b_4 + b_5\right) t^{12} + O\left(t^{14}\right) \\
\frac{\omega_2}{dt} &= 1 + b_1 t^2 + \left(b_1^2 + 2 b_2\right) t^4 + \left(b_1^3 + 6 b_1 b_2 + 3 b_3\right) t^6 + \left(b_1^4 + 6 b_2^2 + 12 b_1^2 b_2 + 12 b_1 b_3 + 4 b_4\right) t^8 \\
&\qquad\qquad + \left(b_1^5 + 30 b_1 b_2^2 + 20 b_1^3 b_2 + 30 b_1^2 b_3 + 20 b_2 b_3 + 20 b_1 b_4 + 5 b_5\right) t^{10} + O\left(t^{12}\right) \\
\zeta_1 &= \frac{1}{t^3} + \alpha t + \delta t^3 + O\left(t^5\right) \\
\zeta_2 &= \frac{1}{t} + \beta t + \gamma t^3 + O\left(t^5\right) \\
\frac{d\zeta_1}{\omega_1} &= -3 x^3 - 3 b_1 x^2 + \alpha x + (3 b_1 b_2 - b_1 \alpha + 3 b_3 + 3 \delta) \\
\frac{d\zeta_2}{\omega_1} &= -x^2 + \beta x + (b_2 - b_1 \beta + 3 \gamma)
\end{aligned}
$$

(Computed with Mathematica)

Chapter 4

Jacobians of curves of genus two

4.1 Preliminaries on curves and Jacobians

4.1.1 Jacobians

For reference, see Milne [35]. To any curve C over an algebraically closed field k, we have the group $\mathrm{Div}(C)$ of divisors on C. By definition, $\mathrm{Div}(C)$ is the group of formal finite $\mathbb{Z}$-linear sums of points on C. There is a group homomorphism, called the degree map, $\deg : \mathrm{Div}(C) \to \mathbb{Z}$ defined by taking an element $\sum n_P P$ to the sum of the coefficients $\sum n_P$ (note that all but finitely many n_p are zero). The kernel of the degree map is denoted $\mathrm{Div}^0(C)$. Any meromorphic function f on C has an associated divisor $(f) = \sum n_P P$ where the n_P is the order of vanishing of f at the point P (positive if f vanishes at P, negative if f has a pole at P, zero otherwise). Such a divisor is said to be a principal divisor.

In the case that C is smooth and projective, all principal divisors have degree zero, and thus form a subgroup of $\mathrm{Div}^0(C)$. Two divisors D_1 and D_2 which differ by a principal divisor are said to be linearly equivalent, which we denote by $D_1 \sim D_2$. The quotient of $\mathrm{Div}(C)$ by linear equivalence is called the Picard group of C, denoted $\mathrm{Pic}(C)$. Similarily, the subgroup of $\mathrm{Pic}(C)$ given by the quotient of $\mathrm{Div}^0(C)$ by the principal divisors is denoted $\mathrm{Pic}^0(C)$. The group $\mathrm{Pic}^0(C)$ can be naturally represented as the functor of points of an abelian variety, called the Jacobian of C, denoted also by $\mathrm{Jac}(C)$. The dimension of $\mathrm{Jac}(C)$ is precisely the genus of C.

Let the genus of C be at least one. Given the choice of a point Q on C, there is a morphism, called the Abel-Jacobi map, $C \to \mathrm{Jac}(C)$ defined by taking a point P and sending it to the class of $P - Q$. This map on points gives rise to an embedding of C into $\mathrm{Jac}(C)$ as varieties. We then get maps $C^n \to \mathrm{Jac}(C)$ by adding the images of n points in $\mathrm{Jac}(C)$. As $\mathrm{Jac}(C)$ is an abelian group, this map descends to the symmetric power $C^{(n)}$. If C is genus g, then the map $\Phi : C^{(g)} \to \mathrm{Jac}(C)$ is surjective and birational. The image $C^{(g-1)} \to \mathrm{Jac}(C)$ is an effective divisor Θ on $\mathrm{Jac}(C)$ which induces a principal polarization.

4.1.2 Symmetric powers of curves

The fact that $C^{(g)}$ and $\mathrm{Jac}(C)$ are birational allows us to describe explicitly the function theory of $\mathrm{Jac}(C)$ via functions on $C^{(g)}$ which are ultimately given in terms of functions on C.

We will be primarily interested in the case where C is a smooth projective curve of genus 2. If the characteristic of the field is not 2 and we assume further that C has a rational Weierstrass point, we can always write C to have an affine model given by

$$y^2 = x^5 + b_1x^4 + b_2x^3 + b_3x^2 + b_4x + b_5$$

where the quintic has distinct roots. Under this model, the unique point of C at infinity, denoted by ∞, will be the prescribed rational Weierstrass point. The hyperelliptic involution ι is given on this model by $(x, y) \mapsto (x, -y)$. We will use ∞ as the base point for the Abel-Jacobi map.

Inside $C \times C$ we have the divisors M_1 consisting of all points (∞, P) and M_2 consisting of the points (P, ∞). Define the divisor E consisting of all points $(P, \iota P)$ and define Δ to be the divisor consisting of points (P, P). Then if $M = M_1 + M_2$, we have M, Δ and E are invariant under S_2 and thus descend to divisors (still denoted M, Δ and E) on $C^{(2)}$.

Since ∞ is a Weierstrass point of C, a pair of points P, Q in C are linearly equivalent to 2∞ exactly when $Q = \iota P$. This means that the fiber $\Phi^{-1}(0) = E$. On the other hand, if $\Phi(P_1 + P_2) = \Phi(Q_1 + Q_2)$, then $P_1 + P_2 \sim Q_1 + Q_2$ so $P_1 + P_2 + \iota Q_1 + \iota Q_2 \sim 4\infty$. Then there is a function f in $\mathscr{L}(4\infty)$ vanishing precisely on $P_1, P_2, \iota Q_1, \iota Q_2$, but since $\mathscr{L}(4\infty)$ is spanned by 1, x and x^2, we see that f must be a polynomial in x and hence has zeroes which are conjugate under ι.

This is only possible if the ιQ_i are a permutation of the ιP_i (and hence the Q_i are a permuatation of the P_i) or if $P_1 = \iota P_2$ and $Q_1 = \iota Q_2$. This means that Φ is injective on $C^{(2)} - E$.

Points on M are of the form $P + \infty$ and so have image $\Phi(P + \infty) = P + \infty - 2\infty = P - \infty$. This is precisely the image of P under the Abel-Jacobi map. We see that the image of M under Φ is exactly Θ (which contains the identity as the image of $\infty + \infty$). Thus the pullback of Θ is some positive combination of M and E.

Make the following definitions

$$\wp_{11} = \frac{(x_1 + x_2)(x_1x_2)^2 + 2b_1(x_1x_2)^2 + b_2(x_1 + x_2)(x_1x_2) + 2b_3(x_1x_2) + b_4(x_1 + x_2) + 2b_5 - 2y_1y_2}{(x_1 - x_2)^2}$$

$$\wp_{12} = -x_1x_2$$

$$\wp_{22} = x_1 + x_2$$

$$\wp_{111} = 2\frac{y_2\varphi(x_1, x_2) - y_1\varphi(x_2, x_1)}{(x_1 - x_2)^3}$$

$$\varphi(x_1, x_2) = (3x_1 + x_2)x_1^3x_2 + 4b_1x_1^3x_2 + b_2(x_1 + 3x_2)x_1^2 + 2b_3(x_1 + x_2)x_1 + b_4(3x_1 + x_2) + 4b_5$$

$$\wp_{112} = 2\frac{y_1x_2^2 - y_2x_1^2}{x_1 - x_2}$$

$$\wp_{122} = -2\frac{y_1x_2 - y_2x_1}{x_1 - x_2}$$

$$\wp_{222} = 2\frac{y_1 - y_2}{x_1 - x_2}$$

$$\wp = \wp_{11}\wp_{22} - \wp_{12}^2.$$

These functions mimic the complex theory of genus two curves, cf ([4] page 38) and ([19] page 99).

We have a standard choice of holomorphic differentials on C given by $\omega_1 = \frac{dx}{2y}$ and $\omega_2 = \frac{xdx}{2y}$. By pulling back along the projection maps $p_1, p_2 : C^2 \to C$, we get holomorphic differentials $p_i^*\omega_j$. Adding these together, we get differentials $\Omega_j = p_1^*\omega_j + p_2^*\omega_j$ which are symmetric under the action of S_2 and so descend to holomorphic differentials on $C^{(2)}$. This induces a pair of derivations on the function field of $C^{(2)}$ by the rule

$$df = (D_1f)\Omega_1 + (D_2f)\Omega_2.$$

Lemma 30. *If $\overline{d}$ is the derivation on the function field of C given by $\frac{d}{\omega_1} = \frac{2yd}{dx}$, then*

$$\begin{aligned} D_1 &= \frac{x_1\overline{d}_2 - x_2\overline{d}_1}{x_1 - x_2} \\ D_2 &= \frac{\overline{d}_1 - \overline{d}_2}{x_1 - x_2}. \end{aligned}$$

Proof.

$$\begin{aligned}
&\frac{x_1\overline{d}_2 - x_2\overline{d}_1}{x_1 - x_2} f\left(\frac{dx_1}{2y_1} + \frac{dx_2}{2y_2}\right) + \frac{\overline{d}_1 - \overline{d}_2}{x_1 - x_2} f\left(\frac{x_1dx_1}{2y_1} + \frac{x_2dx_2}{2y_2}\right) \\
&= \frac{x_1\overline{d}_2 f - x_2\overline{d}_1 f}{x_1 - x_2}\left(\frac{dx_1}{2y_1} + \frac{dx_2}{2y_2}\right) + \frac{\overline{d}_1 f - \overline{d}_2 f}{x_1 - x_2}\left(\frac{x_1dx_1}{2y_1} + \frac{x_2dx_2}{2y_2}\right) \\
&= \frac{1}{2y_1y_2(x_1-x_2)}\Big(\left(x_1\overline{d}_2 f - x_2\overline{d}_1 f\right)\left(y_2dx_1 + y_1dx_2\right) + \left(\overline{d}_1 f - \overline{d}_2 f\right)\left(y_2x_1dx_1 + y_1x_2dx_2\right)\Big) \\
&= \frac{1}{2y_1y_2(x_1-x_2)}\Big((x_1y_2\overline{d}_2 f - x_2y_2\overline{d}_1 f + x_1y_2\overline{d}_1 f - x_1y_2\overline{d}_2 f)dx_1 \\
&\qquad\qquad + (x_1y_1\overline{d}_2 f - x_2y_1\overline{d}_1 f + x_2y_1\overline{d}_1 f - x_2y_1\overline{d}_2 f)dx_2\Big) \\
&= \frac{1}{2y_1y_2(x_1-x_2)}\Big((-x_2y_2\overline{d}_1 f + x_1y_2\overline{d}_1 f)dx_1 + (x_1y_1\overline{d}_2 f - x_2y_1\overline{d}_2 f)dx_2\Big) \\
&= \frac{1}{2y_1y_2(x_1-x_2)}\Big((x_1 - x_2)y_2\overline{d}_1 f dx_1 + (x_1 - x_2)y_1\overline{d}_2 f dx_2\Big) \\
&= \frac{1}{2y_1y_2(x_1-x_2)}\left(2(x_1 - x_2)y_1y_2\frac{d}{dx_1} f dx_1 + 2(x_1 - x_2)y_1y_2\frac{d}{dx_2} f dx_2\right) \\
&= \frac{df}{dx_1}dx_1 + \frac{df}{dx_2}dx_2 \\
&= df.
\end{aligned}$$

□

Direct calculation yields $D_1\wp_{ij} = \wp_{1ij}$ and $D_2\wp_{ij} = \wp_{ij2}$ for each $\wp_{ij}$.

Lemma 31. *The functions 1, $\wp_{11}$, $\wp_{12}$, and $\wp_{22}$ form a basis of $\mathscr{L}(2\Theta)$. The functions 1, $\wp_{11}$, $\wp_{12}$, $\wp_{22}$, $\wp_{111}$, $\wp_{112}$, $\wp_{122}$, $\wp_{222}$, and $\wp$ form a basis of $\mathscr{L}(3\Theta)$.*

Proof. Since x and y are regular away from ∞, the numerators of $\wp_{ij}$ and $\wp_{ijk}$ are regular away from Θ. In particular $\wp_{12}$ and $\wp_{22}$ are regular away from M.

To check $\wp_{222}$, if we let $f(x) = x^5 + b_1x^4 + b_2x^3 + b_3x^2 + b_4x + b_5$, we observe

$$\wp_{222} = 2\frac{y_1 - y_2}{x_1 - x_2} = 2\frac{y_1^2 - y_2^2}{(x_1 - x_2)(y_1 + y_2)} = \frac{2}{y_1 + y_2}\frac{f(x_1) - f(x_2)}{x_1 - x_2}.$$

Since $f(x_1) - f(x_2)$ is divisble by $x_1 - x_2$, any pole of $\wp_{222}$ must be contained in the zero locus $V(x_1 - x_2, y_1 + y_2)$, which is E. Hence $\wp_{222}$ is regular away from Θ.

Similarily for $\wp_{122}$, we see

$$\wp_{122} = 2\frac{y_1x_2 - y_2x_1}{x_1 - x_2} = 2\frac{x_1y_1y_2 - x_2y_1y_2 + x_1y_2^2 - x_2y_1^2}{(x_1 - x_2)(y_1 + y_2)} = \frac{2}{y_1 + y_2}\left(y_1y_2 + \frac{x_1f(x_2) - x_2f(x_1)}{x_1 - x_2}\right).$$

As before, $x_1 - x_2$ divides $x_1f(x_2) - x_2f(x_1)$, so $\wp_{122}$ is regular off Θ.

Direct calculation yields the equations

$$\begin{aligned}
\wp_{112} &= \wp_{12}\wp_{222} - \wp_{22}\wp_{122} \\
\wp_{11} &= \frac{1}{4}\wp_{222}^2 - \wp_{22}^3 - \wp_{12}\wp_{22} - b_1\wp_{22}^2 - b_3 \\
\wp_{111} &= 2\wp_{22}\wp_{112} - \wp_{12}\wp_{122} - \wp_{11}\wp_{222} + 2b_1\wp_{112} - b_2\wp_{122}
\end{aligned}$$

which express each of $\wp_{112}$, $\wp_{11}$, and $\wp_{111}$ in terms of functions which are regular away from Θ. When paired with the definition $\wp = \wp_{11}\wp_{22} - \wp_{12}^2$, we see that all of the claimed functions are regular away from Θ.

To compute the order of a function f along Θ, by ([2] Lemma 1) one can compute the order of vanishing at ∞ of f when viewing x_2 and y_2 as generic values. It follows that 1 is in $\mathscr{L}(0)$, that $\wp_{11}, \wp_{12}, \wp_{22}$ are in $\mathscr{L}(2\Theta) - \mathscr{L}(\Theta)$ and that $\wp_{111}, \wp_{112}, \wp_{122}, \wp_{222}, \wp$ are in $\mathscr{L}(3\Theta) - \mathscr{L}(2\Theta)$.

Taking $\frac{\wp_{11}}{\wp_{22}}$, $\frac{\wp_{12}}{\wp_{22}}$ and $\frac{\wp_{22}}{\wp_{22}} = 1$ and restricting them to M, then on the element $P + \infty$, they evaluate to $x^2(P)$, $-x(P)$ and $1(P)$ respectively. Since 1, x, and x^2 are linearly independent on C, these must be linearly independent. At the same time, $\frac{1}{\wp_{22}}$ restricts to the zero function on M, so if it were a linear combination of the $\wp_{ij}$, it would have to be with all zero coefficients. On the other hand, the Riemann–Roch Theorem for abelian surfaces implies that $\ell(n\Theta) = n^2$ so $\mathscr{L}(\Theta)$ is dimension one and $\mathscr{L}(2\Theta)$ is dimension four, so they have bases 1 and $\{1, \wp_{11}, \wp_{12}, \wp_{22}\}$, respectively. Similarily, $\frac{\wp_{111}}{\wp_{222}}$, $\frac{\wp_{112}}{\wp_{222}}$, $\frac{\wp_{122}}{\wp_{222}}$, $\frac{\wp_{222}}{\wp_{222}}$, and $\frac{\wp}{\wp_{222}}$ restricted to M become $-x^3$, x^2, $-x$, 1, and

$-y$, respectively, while any element of $\mathscr{L}(2\Theta)$ divided by $\wp_{222}$ restricted to M becomes zero, so $\wp_{111}$, $\wp_{112}$, $\wp_{122}$, $\wp_{222}$, and $\wp$ must be a basis of $\mathscr{L}(3\Theta)/\mathscr{L}(2\Theta)$. □

A generalized theorem of Lefschetz ([46] Theorem in section 17) says that $\mathscr{L}(3\Theta)$ is very ample, hence its sections induce an embedding into projective space $\mathrm{Jac}(C) \to \mathbb{P}^8$. This embedding and the resulting equations defining $\mathrm{Jac}(C)$ are given explicitly in [19].

For reference, we define the functions

$$\wp_{1111} = 6\wp_{11}^2 + 4b_3\wp_{11} + 4b_4\wp_{12} - 12b_5\wp_{22} - 8b_1b_5 + 2b_2b_4, \tag{4.1}$$

$$\wp_{1112} = 6\wp_{11}\wp_{12} + 4b_3\wp_{12} - 2b_4\wp_{22} - 4b_5, \tag{4.2}$$

$$\wp_{1122} = 6\wp_{11}\wp_{22} - 4\wp + 2b_2\wp_{12}, \tag{4.3}$$

$$\wp_{1222} = 6\wp_{12}\wp_{22} - 2\wp_{11} + 4b_1\wp_{12}, \tag{4.4}$$

$$\wp_{2222} = 6\wp_{22}^2 + 4\wp_{12} + 4b_1\wp_{22} + 2b_2. \tag{4.5}$$

Direct calculation (via Mathematica, say) shows $D_1\wp_{ijk} = \wp_{1ijk}$ and $D_2\wp_{ijk} = \wp_{ijk2}$ for each $\wp_{ijk}$.

We follow [19] and define

$$\begin{aligned}
X_{11} &= \wp_{11} & X_{111} &= \frac{1}{2}\wp_{111} \\
X_{12} &= \wp_{12} & X_{112} &= \frac{1}{2}\wp_{112} \\
X_{22} &= \wp_{22} & X_{122} &= \frac{1}{2}\wp_{122} \\
X &= \frac{1}{2}\left(\wp + b_2\wp_{12} - b_4\right) & X_{222} &= \frac{1}{2}\wp_{222}.
\end{aligned}$$

Note that the factors of $\frac{1}{2}$ are analagous to the difference between $\wp'$ and y in the standard Weierstrass affine model $y^2 = x^3 + Ax + B$ for an elliptic curve over $\mathbb{C}$. In [19], the equations defining the Jacobian of C are explicitly written down in terms of these functions.

Lemma 32. *The functions $T_1 = -\frac{X_{11}}{X_{111}}$ and $T_2 = -\frac{X}{X_{111}}$ descend to a pair of regular local parameters at the origin of $\mathrm{Jac}(C)$ with T_1 vanishing along Θ (to order 1).*

Proof. See [19] Theorem 4.2. □

The X_{ij} and X_{ijk} are all expressed in terms of the x_i and y_i, and thus have expansions in terms of t_1 and t_2. In fact, these expansions must be invariant under the action of S_2, hence must be in terms of $s_1 = t_1t_2$ and $s_2 = t_1 + t_2$. A priori, these expansions have coefficients in $\mathbb{Q}(b_1, \ldots, b_5)$. We will check the t expansions of the various pieces. We have

$$x_1 - x_2 = \frac{1}{t_1^2} - \frac{1}{t_2^2} + \cdots = \frac{1}{t_1^2t_2^2}\left(t_2^2 - t_1^2 + O(\deg \geq 4)\right)$$

with coefficients in $\mathbb{Z}[b_1, \ldots, b_5]$. The higher terms are of the form $t_1^{2k} - t_2^{2k}$ which are all divisible by $t_1^2 - t_2^2$, so in fact

$$x_1 - x_2 = \frac{(t_1 - t_2)(t_1 + t_2)}{t_1^2t_2^2}\left(-1 + O(\deg \geq 2)\right)$$

reflecting the fact that $x_1 - x_2$ has divisor $E + \Delta - 2M_1 - 2M_2$ on C^2 ($x_1 - x_2$ vanishes exactly along E and Δ while having poles along M_1 and M_2, all of which include (∞, ∞), so to check the orders of vanishing it suffices to see the expansion in terms of t_1 and t_2, from which the vanishing orders can be read off). The numerator of X_{11} is given by

$$\begin{aligned}
&(x_1 + x_2)(x_1x_2)^2 + 2b_1(x_1x_2)^2 + b_2(x_1 + x_2)(x_1x_2) + 2b_3(x_1x_2) + b_4(x_1 + x_2) + 2b_5 - 2y_1y_2 \\
&= \left(\frac{1}{t_1^2} + \frac{1}{t_2^2} + \cdots\right)\left(\frac{1}{t_1^4t_2^4} + \cdots\right) + 2b_1\left(\frac{1}{t_1^4t_2^4} + \cdots\right) + b_2\left(\frac{1}{t_1^2} + \frac{1}{t_2^2} + \cdots\right)\left(\frac{1}{t_1^2t_2^2} + \cdots\right) \\
&+ 2b_3\left(\frac{1}{t_1^2t_2^2} + \cdots\right) + b_4\left(\frac{1}{t_1^2} + \frac{1}{t_2^2} + \cdots\right) + 2b_5 - 2\left(\frac{1}{t_1^5t_2^5} + \cdots\right) \\
&= \frac{1}{t_1^6t_2^6}\left(t_2^2 + t_1^2 - 2t_1t_2 + O(\deg \geq 4)\right) \\
&= \frac{1}{t_1^6t_2^6}\left((t_2 - t_1)^2 + O(\deg \geq 4)\right)
\end{aligned}$$

with all coefficients in $\mathbb{Z}[b_1, \ldots, b_5]$. Since X_{11} does not have a pole along Δ, $(t_1 - t_2)^2$ must divide the entire numerator yielding an expansion

$$\frac{(t_1 - t_2)^2}{t_1^6t_2^6}\left(1 + O(\deg \geq 2)\right).$$

We see then that X_{11} has an expansion

$$\begin{aligned}
X_{11} &= \frac{(t_1 - t_2)^2}{t_1^6t_2^6}\left(1 + O(\deg \geq 2)\right)\left(\frac{(t_1 - t_2)(t_1 + t_2)}{t_1^2t_2^2}\left(-1 + O(\deg \geq 2)\right)\right)^{-2} \\
&= \frac{1}{t_1^2t_2^2(t_1 + t_2)^2}\left(1 + O(\deg \geq 2)\right)
\end{aligned}$$

with coefficients in $\mathbb{Z}[b_1, \ldots, b_5]$.

The t expansion of $\varphi(x_1, x_2)$ is given by

$$\begin{aligned}
&(3x_1 + x_2)x_1^3x_2 + 4b_1x_1^3x_2 + b_2(x_1 + 3x_2)x_1^2 + 2b_3(x_1 + x_2)x_1 + b_4(3x_1 + x_2) + 4b_5 \\
&= \left(\frac{3}{t_1^2} + \frac{1}{t_2^2} + \cdots\right)\left(\frac{1}{t_1^2} + \cdots\right)^3\left(\frac{1}{t_2^2} + \cdots\right) + 4b_1\left(\frac{1}{t_1^2} + \cdots\right)^3\left(\frac{1}{t_2^2} + \cdots\right) \\
&\qquad\qquad + b_2\left(\frac{1}{t_1^2} + \frac{3}{t_2^2} + \cdots\right)\left(\frac{1}{t_1^2} + \cdots\right)^2 + 2b_3\left(\frac{1}{t_1^2} + \frac{1}{t_2^2} + \cdots\right)\left(\frac{1}{t_1^2} + \cdots\right) \\
&\qquad\qquad + b_4\left(\frac{3}{t_1^2} + \frac{1}{t_2^2} + \cdots\right) + 4b_5 \\
&= \frac{1}{t_1^8t_2^4}\left(t_1^2 + 3t_2^2 + \cdots\right) + 4b_1\left(\frac{1}{t_1^6t_2^2} + \cdots\right) + \frac{b_2}{t_1^6t_2^2}\left(3t_1^2 + t_2^2 + \cdots\right) + \frac{2b_3}{t_1^4t_2^2}\left(t_1^2 + t_2^2 + \cdots\right) \\
&\qquad\qquad + \frac{b_4}{t_1^2t_2^2}\left(t_1^2 + 3t_2^2 + \cdots\right) + 4b_5 \\
&= \frac{1}{t_1^8t_2^4}\left(t_1^2 + 3t_2^2 + O(\deg \geq 4)\right)
\end{aligned}$$

with coefficients in $\mathbb{Z}[b_1, \ldots, b_5]$, so X_{111} has numerator

$$\begin{aligned}
&y_2\varphi(x_1, x_2) - y_1\varphi(x_2, x_1) \\
&\qquad = \left(-\frac{1}{t_2^5} + O(t_2^{-3})\right)\frac{1}{t_1^8t_2^4}\left(t_1^2 + 3t_2^2 + O(\deg \geq 4)\right) \\
&\qquad\qquad\qquad - \left(-\frac{1}{t_1^5} + O(t_1^{-3})\right)\frac{1}{t_1^4t_2^8}\left(3t_1^2 + t_2^2 + O(\deg \geq 4)\right) \\
&\qquad = \frac{-1}{t_1^8t_2^9}\left(t_1^2 + 3t_2^2 + O(\deg \geq 4)\right) + \frac{1}{t_1^9t_2^8}\left(3t_1^2 + t_2^2 + O(\deg \geq 4)\right) \\
&\qquad = \frac{1}{t_1^9t_2^9}\left(t_2^3 + 3t_1^2t_2 - t_1^3 - 3t_1t_2^2 + O(\deg \geq 5)\right) \\
&\qquad = \frac{1}{t_1^9t_2^9}\left((t_2 - t_1)^3 + O(\deg \geq 5)\right).
\end{aligned}$$

The numerator of X_{111} has lead term

$$\frac{-1}{t_1^9t_2^9}\left((t_1 - t_2)^3 + O(\deg \geq 5)\right)$$

and because X_{111} also does not have a pole along Δ, its numerator must be divisible by $(t_1 - t_2)^3$

and therefore

$$\begin{aligned} X_{111} &= -\frac{(t_1-t_2)^3}{t_1^9t_2^9}\left(1+O(\deg\geq 2)\right)\left(\frac{(t_1-t_2)(t_1+t_2)}{t_1^2t_2^2}\left(-1+O(\deg\geq 2)\right)\right)^{-3} \\ &= \frac{-1}{t_1^3t_2^3(t_1+t_2)^3}\left(1+O(\deg\geq 2)\right) \end{aligned}$$

with coefficients in $\mathbb{Z}[b_1,\ldots,b_5]$.

Hence we have $T_1 = -\frac{X_{11}}{X_{111}}$ has an expansion

$$\begin{aligned} T_1 &= \frac{1}{t_1^2t_2^2(t_1+t_2)^2}\left(1+O(\deg\geq 2)\right)\left(\frac{1}{t_1^3t_2^3(t_1+t_2)^3}\left(1+O(\deg\geq 2)\right)\right)^{-1} \\ &= t_1t_2(t_1+t_2)(1+O(\deg\geq 2)) \end{aligned} \tag{4.6}$$

with all coefficients in $\mathbb{Z}[b_1,\ldots,b_5]$.

Expanding X in terms of x_1,x_2,y_1,y_2, we have

$$\begin{aligned} X = \frac{1}{(x_1-x_2)^2}\Big(&2(x_1x_2)^3 + b_1(x_1+x_2)(x_1x_2)^2 + 2b_2(x_1x_2)^2 + b_3(x_1+x_2)x_1x_2 \\ &+ 2b_4(x_1x_2) + b_5(x_1+x_2) - y_1y_2(x_1+x_2)\Big) \end{aligned}$$

so the t-expansion of the numerator is

$$\begin{aligned} &2(x_1x_2)^3 + b_1(x_1+x_2)(x_1x_2)^2 + 2b_2(x_1x_2)^2 + b_3(x_1+x_2)x_1x_2 \\ &\qquad + 2b_4(x_1x_2) + b_5(x_1+x_2) - y_1y_2(x_1+x_2) \\ &= 2\left(\frac{1}{t_1^6t_2^6}+\cdots\right) + b_1\left(\frac{1}{t_1^2}+\frac{1}{t_2^2}+\cdots\right)\left(\frac{1}{t_1^4t_2^4}+\cdots\right) + 2b_2\left(\frac{1}{t_1^4t_2^4}+\cdots\right) \\ &\qquad + b_3\left(\frac{1}{t_1^2}+\frac{1}{t_2^2}+\cdots\right)\left(\frac{1}{t_1^2t_2^2}+\cdots\right) + 2b_4\left(\frac{1}{t_1^2t_2^2}+\cdots\right) \\ &\qquad + b_5\left(\frac{1}{t_1^2}+\frac{1}{t_2^2}+\cdots\right) - \left(\frac{1}{t_1^5t_2^5}+\cdots\right)\left(\frac{1}{t_1^2}+\frac{1}{t_2^2}+\cdots\right) \\ &= \frac{1}{t_1^7t_2^7}\left(2t_1t_2 - t_1^2 - t_2^2 + O(\deg\geq 4)\right) \\ &= \frac{-1}{t_1^7t_2^7}\left((t_1-t_2)^2 + O(\deg\geq 4)\right) \end{aligned}$$

with all coefficients in $\mathbb{Z}[b_1,\ldots,b_5]$. As with X_{11}, X does not have a pole along Δ, so $(t_1-t_2)^2$ must divide the whole numerator, giving

$$\frac{-(t_1-t_2)^2}{t_1^7t_2^7}\left(1+O(\deg\geq 2)\right).$$

Dividing by the denominator, we get that X has an expansion

$$\begin{aligned} X &= \frac{-(t_1-t_2)^2}{t_1^7t_2^7}\left(1+O(\deg\geq 2)\right)\left(\frac{(t_1-t_2)(t_1+t_2)}{t_1^2t_2^2}\left(-1+O(\deg\geq 2)\right)\right)^{-2} \\ &= \frac{-1}{t_1^3t_2^3(t_1+t_2)^2}\left(1+O(\deg\geq 2)\right) \end{aligned}$$

with coefficients in $\mathbb{Z}[b_1,\ldots,b_5]$.

At last, we see that $T_2 = -\frac{X}{X_{111}}$ has an expansion

$$\begin{aligned} T_2 &= -\frac{-1}{t_1^3t_2^3(t_1+t_2)^2}\left(1+O(\deg\geq 2)\right)\left(\frac{-1}{t_1^3t_2^3(t_1+t_2)^3}\left(1+O(\deg\geq 2)\right)\right)^{-1} \\ &= -(t_1+t_2)(1+O(\deg\geq 2)) \end{aligned} \tag{4.7}$$

with all coefficients in $\mathbb{Z}[b_1,\ldots,b_5]$.

4.2 p-Adic Weierstrass sigma function in dimension two

We will work in the setting where K is a p-adic field (characteristic zero with residue characteristic p) with ring of integers R and residue field k and C is a smooth projective curve of genus two with affine model

$$y^2 = x^5 + b_1x^4 + b_2x^3 + b_3x^2 + b_4x + b_5.$$

Then $\mathrm{Jac}(C)$ is a two dimensional abelian variety birational to $C^{(2)}$. Embedding C into $\mathrm{Jac}(C)$ via the Abel-Jacobi map with ∞ as basepoint, we get an explicit surjective birational map $C^{(2)} \to \mathrm{Jac}(C)$. The image of C under this map is a symmetric theta divisor Θ in $\mathrm{Jac}(C)$. We will further require that the H_1 be invertible in R, which forces the Jacobian to have ordinary reduction (see [27] for reference).

Under this identification, we can be more explicit with the functions appearing in Chapter 2. We can use T_1 and T_2 as odd local parameters to the origin of $\mathrm{Jac}(C)$. In particular, we can use T_1 as a function representing Θ at the origin, taking it as our choice of g in $\sigma = \sigma_g$, which implies in particular that $\sigma = T_1 \cdot u$ for a power series $u(T_1, T_2)$ with lead term 1. Since T_1 is odd, Θ must be an odd symmetric theta divisor, hence σ must also be odd. We thus have

$$\sigma = \sum_{\substack{i>1\\ j\geq 0}} a_{i,j} T_1^i T_2^j = T_1 + O(\deg \geq 3).$$

Recall the four maps $m, s, p_1, p_2 : \mathrm{Jac}(C) \times \mathrm{Jac}(C) \to \mathrm{Jac}(C)$ defined by $m(u,v) = u + v$, $s(u,v) = u - v$, $p_1(u,v) = u$, and $p_2(u,v) = v$. In Proposition 17 we found that if u, v are in $\mathrm{Jac}(C)^f$, then $\frac{\sigma(u+v)\sigma(u-v)}{\sigma(u)^2\sigma(v)^2}$ was the restriction of a rational function on $\mathrm{Jac}(C) \times \mathrm{Jac}(C)$ with a particular divisor, but now we can specify the function itself.

Proposition 33. *For u, v in the kernel of reduction of* $\mathrm{Jac}(C)$*,*

$$\frac{\sigma(u+v)\sigma(u-v)}{\sigma(u)^2\sigma(v)^2} = X_{11}(v) - X_{11}(u) + X_{12}(u)X_{22}(v) - X_{12}(v)X_{22}(u).$$

Proof. By [2], the right hand side has divisor $m^*\Theta + s^*\Theta - 2p_1^*\Theta - 2p_2\Theta$, so by Proposition 17 we have

$$\frac{\sigma(u+v)\sigma(u-v)}{\sigma(u)^2\sigma(v)^2} = c\left(X_{11}(v) - X_{11}(u) + X_{12}(u)X_{22}(v) - X_{12}(v)X_{22}(u)\right)$$

for some nonzero constant c. Clearing the denomenator, we see

$$\sigma(u+v)\sigma(u-v) = c \cdot \sigma(u)^2\sigma(v)^2\left(X_{11}(v) - X_{11}(u) + X_{12}(u)X_{22}(v) - X_{12}(v)X_{22}(u)\right). \tag{4.8}$$

As power series in T_1 and T_2

$$m^*T_1 = T_1^u + T_1^v + O(\deg \geq 3)$$

$$m^*T_2 = T_2^y + T_2^v + O(\deg \geq 3)$$

$$s^*T_1 = T_1^u - T_1^v + O(\deg \geq 3)$$

$$s^*T_2 = T_2^u - T_2^v + O(\deg \geq 3)$$

(all terms are odd degree because T_1 and T_2 are both odd under $[-1]^*$). We see

$$m^*\sigma = \sum_{\substack{i>1\\ j\geq 0}} a_{i,j} m^*T_1^i m^*T_2^j = m^*T_1 + O(\deg \geq 3) = T_1^u + T_1^v + O(\deg \geq 3).$$

Similarily

$$s^*\sigma = T_1^u - T_1^v + O(\deg \geq 3)$$

$$p_1^*\sigma = T_1^u + O(\deg \geq 3)$$

$$p_2^*\sigma = T_1^v + O(\deg \geq 3).$$

The lead term on the left hand side of (4.8) is given by

$$(m^*\sigma)(s^*\sigma) = (T_1^u + T_1^v + O(\deg \geq 3))(T_1^u - T_1^v + O(\deg \geq 3)) = (T_1^u)^2 - (T_1^v)^2 + O(\deg \geq 4).$$

Using the formulas in the proof of [19] Theorem 4.2, we have

$$X_{22} = T_1^{-2}(2T_1T_2 + O(\deg \geq 4))$$

$$X_{12} = T_1^{-2}(-T_2^2 + O(\deg \geq 4))$$

$$X_{11} = T_1^{-2}(1 + O(\deg \geq 2)).$$

So the right hand side of (4.8) is given by

$$\begin{aligned}
& c \cdot p_1^*\sigma^2 p_2^*\sigma^2 \left(p_2^*X_{11} - p_1^*X_{11} + p_1^*X_{12}p_2^*X_{22} - p_2^*X_{12}p_1^*X_{22}\right) \\
&= c \cdot \left((T_1^u)^2(T_1^v)^2 + O(\deg \geq 6)\right) \\
&\times \left((T_1^v)^{-2} - (T_1^u)^{-2} + (T_1^u)^{-2}(T_2^u)^2 2(T_1^v)^{-1}(T_2^v) - (T_1^v)^{-2}(T_2^v)^2 2(T_1^u)^{-1}(T_2^u) + O(\deg \geq 0)\right) \\
&= c \cdot \left((T_1^u)^2(T_1^v)^2 + O(\deg \geq 6)\right)\left((T_1^v)^{-2} - (T_1^u)^{-2} + O(\deg \geq 0)\right) \\
&= c \cdot \left((T_1^u)^2 - (T_1^v)^2 + O(\deg \geq 4)\right).
\end{aligned}$$

And so $c = 1$. □

Proposition 34. *For i, j in $\{1, 2\}$ and u in the kernel of reduction of* $\mathrm{Jac}(C)$,

$$D_iD_j \log(\sigma(u)) = -X_{ij}(u) + c_{ij}$$

for some constants c_{ij} in R.

Proof. Let D_i^u denote the differential operator which acts as D_i with respect to the variable u. In the proof of Proposition 21 at the end of Chapter 2, we saw that

$$(D_i^u - D_i^v)(D_j^u + D_j^v)\log\left(\frac{\sigma(u+v)\sigma(u-v)}{\sigma(u)^2\sigma(v)^2}\right) = 2D_iD_j\log(\sigma(v)) - 2D_iD_j\log(\sigma(u)) \qquad (*)$$

so it would suffice to show

$$(D_i^u - D_i^v)(D_j^u + D_j^v)\log\left(\frac{\sigma(u+v)\sigma(u-v)}{\sigma(u)^2\sigma(v)^2}\right) = 2X_{ij}(u) - 2X_{ij}(v)$$

for various choices of i and j. By Proposition 33, $\frac{\sigma(u+v)\sigma(u-v)}{\sigma(u)^2\sigma(v)^2} = X_{11}(v) - X_{11}(u) + X_{12}(u)X_{22}(v) - X_{12}(v)X_{22}(u)$, so it is actually enough to check

$$0 = (D_i^u - D_i^v)(D_j^u + D_j^v)\log\left(X_{11}(v) - X_{11}(u) + X_{12}(u)X_{22}(v) - X_{12}(v)X_{22}(u)\right) - 2X_{ij}(u) + 2X_{ij}(v).$$

This expression is a rational function in x_1, x_2, y_1, y_2 (symmetric under the action of Σ_2 on the indices) with coefficients in $\mathbb{Q}(b_1, \ldots, b_5)$. This being an algebraic expression in the b_i, it suffices to check it holds over the complex numbers. By [4] p.38, $X_{ij} = -\tilde{D}_i\tilde{D}_j \log(\tilde{\sigma})$ where $\tilde{\sigma}$ is the complex Kleinian sigma function and $\tilde{D}_1$ and $\tilde{D}_2$ are the derivative with respect to complex variables z_1 and z_2, where $(z_1, z_2) = \left(\int \frac{dx_1}{2y_1} + \frac{dx_2}{2y_2}, \int \frac{x_1 dx_1}{2y_1} + \frac{x_2 dx_2}{2y_2}\right)$ in $\mathbb{Q}(b_1, \ldots, b_5)[[T_1, T_2]]$. Since the calculation yielding (*) was purely formal, it also holds replacing σ with $\tilde{\sigma}$ and D_i with $\tilde{D}_i$. But then the desired equality holds for any specialization of C to $\mathbb{C}$ for which the discriminant of $x^5 + b_1x^4 + b_2x^3 + b_3x^2 + b_4x + b_5$ does not vanish (a codimension one condition), so it must hold as an algebraic identity.

□

4.3 p-Adic Weierstrass zeta functions in dimension two

In analogy to the one dimensional setting, define zeta functions as logarithmic derivative of σ as follows

$$\zeta_{J,1} = \frac{D_1\sigma}{\sigma} \tag{4.9}$$

$$\zeta_{J,2} = \frac{D_2\sigma}{\sigma}. \tag{4.10}$$

In this section we will explore the connection between $\zeta_{J,i}$ and $\zeta_{C,i}$. In the process we will compute the c_{ij} of Proposition 34 in terms of the constants $\alpha, \beta, \delta, \gamma$ of Chapter 3 and come to understand how to find the coefficients of σ in its expansion in terms of T_1 and T_2.

By taking sums of $\zeta_{C,i}$ on two copies of C, we define

$$\xi_1 = (\zeta_{C,1})_1 + (\zeta_{C,1})_2 \tag{4.11}$$

$$\xi_2 = (\zeta_{C,2})_1 + (\zeta_{C,2})_2, \tag{4.12}$$

which are a priori elements of the field of fractions of the completion of the local ring $\mathcal{O}_{C^2,(\infty,\infty)}$. Since ξ_1 and ξ_2 are invariant under the action of Σ_2, they descend to the field of fractions of the completion of the local ring $\mathcal{O}_{C^{(2)},2\infty}$. At the same time, pulling back T_1 and T_2 to $C^{(2)}$, they have expansions in terms of $t_1 + t_2$ and $t_1 t_2$ so one could hope to directly compare the ξ_i and the $\zeta_{J.i}$. We start by computing the derivatives of the ξ_i.

Lemma 35. *There is a unique extension of D_1 and D_2 to $\hat{\mathcal{O}}_{C^{(2)},2\infty}$ and hence to its fraction field. With that*

$$\begin{aligned}
D_1\xi_2 &= -\wp_{12} + (b_2 - b_1\beta + 3\gamma)\\
D_2\xi_2 &= -\wp_{22} + \beta\\
D_1\xi_1 &= -\wp_{11} - \frac{1}{2}\wp_{1222} - b_1\wp_{12} + (3b_1b_2 - b_1\alpha + 3b_3 + 3\delta)\\
D_2\xi_1 &= -\wp_{12} - \frac{1}{2}\wp_{2222} - b_1\wp_{22} + \alpha.
\end{aligned}$$

Proof. This is straightforward calculation. We compute

$$\begin{aligned}
D_1\xi_2 &= \frac{x_1\overline{d}_2 - x_2\overline{d}_1}{x_1 - x_2}\left((\zeta_{C,2})_1 + (\zeta_{C,2})_2\right)\\
&= \frac{x_1\overline{d}_2(\zeta_{C,2})_2 - x_2\overline{d}_1(\zeta_{C,2})_1}{x_1 - x_2}\\
&= \frac{x_1(-x_2^2 + \beta x_2 + (b_2 - b_1\beta + 3\gamma)) - x_2(-x_1^2 + \beta x_1 + (b_2 - b_1\beta + 3\gamma))}{x_1 - x_2}\\
&= \frac{(x_1^2x_2 - x_1x_2^2) + (b_2 - b_1\beta + 3\gamma)(x_1 - x_2)}{x_1 - x_2}\\
&= x_1x_2 + (b_2 - b_1\beta + 3\gamma)\\
&= -\wp_{12} + (b_2 - b_1\beta + 3\gamma)
\end{aligned}$$

and

$$\begin{aligned}
D_2\xi_2 &= \frac{\overline{d}_1 - \overline{d}_2}{x_1 - x_2}\left((\zeta_{C,2})_1 + (\zeta_{C,2})_2\right) \\
&= \frac{\overline{d}_1(\zeta_{C,2})_1 - \overline{d}_2(\zeta_{C,2})_2}{x_1 - x_2} \\
&= \frac{(-x_1^2 + \beta x_1 + (b_2 - b_1\beta + 3\gamma)) - (-x_2^2 + \beta x_2 + (b_2 - b_1\beta + 3\gamma))}{x_1 - x_2} \\
&= \frac{-(x_1^2 - x_2^2) + \beta(x_1 - x_2)}{x_1 - x_2} \\
&= -(x_1 + x_2) + \beta \\
&= -\wp_{22} + \beta.
\end{aligned}$$

Similarily

$$\begin{aligned}
D_1\xi_1 &= \frac{x_1\overline{d}_2 - x_2\overline{d}_1}{x_1 - x_2}\left((\zeta_{C,1})_1 + (\zeta_{C,1})_2\right) \\
&= \frac{x_1\overline{d}_2(\zeta_{C,1})_2 - x_2\overline{d}_1(\zeta_{C,1})_1}{x_1 - x_2} \\
&= \frac{1}{x_1 - x_2}\Big(x_1(-3x_2^3 - 3b_1x_2^2 + \alpha x_2 + (3b_1b_2 - b_1\alpha + 3b_3 + 3\delta)) \\
&\qquad\qquad - x_2(-3x_1^3 - 3b_1x_1^2 + \alpha x_1 + (3b_1b_2 - b_1\alpha + 3b_3 + 3\delta))\Big) \\
&= \frac{3(x_1^3x_2 - x_1x_2^3) + 3b_1(x_1^2x_2 - x_2^2x_1) + (3b_1b_2 - b_1\alpha + 3b_3 + 3\delta)(x_1 - x_2)}{x_1 - x_2} \\
&= \frac{3x_1x_2(x_1^2 - x_2^2) + 3b_1x_1x_2(x_1 - x_2) + (3b_1b_2 - b_1\alpha + 3b_3 + 3\delta)(x_1 - x_2)}{x_1 - x_2} \\
&= 3x_1x_2(x_1 + x_2) + 3b_1x_1x_2 + (3b_1b_2 - b_1\alpha + 3b_3 + 3\delta) \\
&= -3\wp_{12}\wp_{22} - 3b_1\wp_{12} + (3b_1b_2 - b_1\alpha + 3b_3 + 3\delta) \\
&= (-3\wp_{12}\wp_{22} + \wp_{11} - 2b_1\wp_{12}) - \wp_{11} - b_1\wp_{12} + (3b_1b_2 - b_1\alpha + 3b_3 + 3\delta) \\
&= -\frac{1}{2}\wp_{1222} - \wp_{11} - b_1\wp_{12} + (3b_1b_2 - b_1\alpha + 3b_3 + 3\delta)
\end{aligned}$$

and

$$\begin{aligned}
D_2\xi_1 &= \frac{\overline{d}_1 - \overline{d}_2}{x_1 - x_2}\left((\zeta_{C,1})_1 + (\zeta_{C,1})_2\right) \\
&= \frac{\overline{d}_1(\zeta_{C,1})_1 - \overline{d}_2(\zeta_{C,1})_2}{x_1 - x_2} \\
&= \frac{1}{x_1 - x_2}\Big((-3x_1^3 - 3b_1x_1^2 + \alpha x_1 + (3b_1b_2 - b_1\alpha + 3b_3 + 3\delta)) \\
&\qquad - (-3x_2^3 - 3b_1x_2^2 + \alpha x_2 + (3b_1b_2 - b_1\alpha + 3b_3 + 3\delta))\Big) \\
&= \frac{-3(x_1^3 - x_2^3) - 3b_1(x_1^2 - x_2^2) + \alpha(x_1 - x_2)}{x_1 - x_2} \\
&= -3(x_1^2 + x_1x_2 + x_2^2) - 3b_1(x_1 + x_2) + \alpha \\
&= -3(\wp_{22}^2 + \wp_{12}) - 3b_1\wp_{22} + \alpha \\
&= (-3\wp_{22}^2 - 2\wp_{12} - 2b_1\wp 22 - b_2) - \wp_{12} - b_1\wp_{22} + \alpha \\
&= -\frac{1}{2}\wp_{2222} - \wp_{12} - b_1\wp_{22} + \alpha.
\end{aligned}$$

□

Recall that σ and hence the $\zeta_{J,i}$ are expressed in terms of T_1 and T_2 with integral coefficients, and that the T_i have expansions in terms of t_1t_2 and $t_1 + t_2$ with coefficients in $\mathbb{Z}[b_1, \ldots, b_5]$. Using this, we are now able to draw a direct comparision between the $\zeta_{J,i}$ and the ξ_i.

Theorem 36. *Interpreted as Laurent series in $s_1 = t_1t_2$ and $s_2 = t_1 + t_2$,*

$$\begin{aligned}
\xi_2 &= \zeta_{J,2} \\
\xi_1 - b_1\xi_2 + \frac{1}{2}\wp_{222} &= \zeta_{J,1}.
\end{aligned}$$

Proof. By Proposition 34 and Lemma 35 we have $D_i(\xi_2 - \zeta_{J,2}) = B_i$ for constants B_1, B_2 and similarily $D_i(\xi_1 - b_1\xi_2 + \frac{1}{2}\wp_{222} - \zeta_{J,1}) = A_i$ for constants A_1, A_2. It suffices to check that there is no nonzero series $F(s_1, s_2)$ such that

$$dF = C_1\Omega_1 + C_2\Omega_2$$

for constants C_1, C_2 (after multiplication by some other constant, we can assume the C_i are in R).

We see

$$dF = C_1\left(\frac{dx_1}{2y_1}+\frac{dx_2}{2y_2}\right)+C_2\left(\frac{x_1dx_1}{2y_1}+\frac{x_2dx_2}{2y_2}\right)=(C_1+C_2x_1)\frac{dx_1}{2y_1}+(C_1+C_2x_2)\frac{dx_2}{2y_2}.$$

Considering this equation as power series in t_1, t_2 (i.e., at the level of C^2), we see $dF(t_1,t_2) = f(t_1)dt_1 + f(t_2)dt_2$ for some Laurent series $f(t)$. Integrating with respect to dt_1 gives $F(t_1,t_2) = G(t_1) + h(t_2)$ for some Laurent series $G(t)$ and $h(t)$ with $G'(t) = f(t)$. Differentiating with respect to t_2 yields $f(t_2) = \frac{\partial}{\partial t_2}F = h'(t_2)$ so integrating again with respect to t_2 yields $F(t_1,t_2) = G(t_1) + G(t_2) + c$ for some constant c (which we can take to be zero by adding $\frac{c}{2}$ to $G(t)$).

Since derivations can only increase pole orders in characteristic 0, we have

$$F(t_1t_2, t_1+t_2) = \sum_{i,j\geq 0}\alpha_{ij}(t_1t_2)^i(t_1+t_2)^j = \sum_{i,j\geq 0}\sum_{\ell=0}^{j}\alpha_{ij}\binom{j}{\ell}t_1^{i+\ell}t_2^{i+j-\ell} = \sum_{r,s\geq 0}\beta_{rs}t_1^rt_2^s$$

where each of the β_{rs} are polynomials in $\mathbb{Z}[\alpha_{ij}]$. In particular, if $F(t_1t_2, t_1+t_2)$ has coefficients with a bounded power of p appearing in the denominators and $F(t_1t_2,t_1+t_2) = G(t_1)+G(t_2)$, so then $G(t)$ has coefficients with a bounded power of p showing up in their denominators because its coefficients are precisely the $\beta_{r0} = \beta_{0s}$. But then $dG(t) = (C_1+C_2x)\frac{dx}{2y}$, which by Lemma 26 forces $C_1 = C_2 = 0$. □

Using the above, we have

Corollary 37. *For* $D_iD_j\log(\sigma) = -\wp_{ij} + c_{ij}$,

$$c_{11} = 3b_1b_2 - b_1\alpha + b_1^2\beta + 3\delta - 3b_1\gamma$$

$$\alpha - b_1\beta = c_{12} = c_{21} = b_2 - b_1\beta + 3\gamma$$

$$c_{22} = \beta$$

so also

$$\alpha = b_2 + 3\gamma.$$

Proof. Bringing together Lemma 35, Theorem 36 and the definition of $\zeta_{J,i}$ we can compute the c_{ij} directly. To find c_{11}, evaluate

$$\begin{aligned} D_1\zeta_{J,1} &= D_1\xi_1 - b_1D_1\xi_2 + \frac{1}{2}D_1\wp_{222} \\ &= \left(-\wp_{11} - \frac{1}{2}\wp_{1222} - b_1\wp_{12} + (3b_1b_2 - b_1\alpha + 3b_3 + 3\delta)\right) \\ &\qquad\qquad - b_1\left(-\wp_{12} + (b_2 - b_1\beta + 3\gamma)\right) + \frac{1}{2}\wp_{1222} \\ &= -\wp_{11} + (3b_1b_2 - b_1\alpha + 3b_3 + 3\delta) - b_1(b_2 - b_1\beta + 3\gamma) \\ &= -\wp_{11} + 3b_1b_2 - b_1\alpha + b_1^2\beta + 3\delta - 3b_1\gamma. \end{aligned}$$

For c_{21}, we find

$$\begin{aligned} D_2\zeta_{J,1} &= D_2\xi_1 - b_1D_2\xi_2 + \frac{1}{2}D_2\wp_{222} \\ &= \left(-\wp_{12} - \frac{1}{2}\wp_{2222} - b_1\wp_{22} + \alpha\right) - b_1\left(-\wp_{22} + \beta\right) + \frac{1}{2}\wp_{2222} \\ &= -\wp_{12} + \alpha - b_1\beta. \end{aligned}$$

Similarily for c_{12}, we get

$$\begin{aligned} D_1\zeta_{J,2} &= D_1\xi_2 \\ &= -\wp_{12} + b_2 - b_1\beta + 3\gamma. \end{aligned}$$

To get c_{22},

$$\begin{aligned} D_2\zeta_{J,2} &= D_2\xi_2 \\ &= -\wp_{22} + \beta. \end{aligned}$$

Finally, note that $D_1D_2\log(\sigma) = D_2D_1\log(\sigma)$ so it must be that $c_{12} = c_{21}$. □

4.4 Future work

In dimension one, the (single) constant analogous to the α, β, δ has an interpretation as the weight two Eisenstein series, a (p-adic) modular form. In the complex theory, Grant [20] shows that the b_i can be interpreted as Siegel modular forms. In future work, we will investigate the role α, β, δ play as p-adic Siegel modular forms in the spirit of [20].

The results of this thesis should force the existence of a universal p-adic sigma function for Jacobians of curves of genus two by taking ξ_2 and computing the anti-logarithmic-derivative, which a priori has coefficients in the field of fractions of $\hat{R}$, and showing that it in fact has coefficients in $\hat{R}$. Then these results may well work for equicharacteristic local fields.

In dimension one, the original interest in p-adic sigma functions was to compute p-adic heights of points on elliptic curves defined over $\mathbb{Q}$. Similarily, the work in this thesis should lend itself well to explicit calculations of p-adic heights for Jacobians of curves of genus two defined over $\mathbb{Q}$.

The theory of Weierstrass ζ functions developed in Chapter 3 for genus two curves generalizes in a straightforward manner to hyperelliptic curves of any genus. There may then also be hope of generalizing this work to hyperelliptic Jacobians in general.

Bibliography

[1] Tom M. Apostol. Modular functions and Dirichlet series in number theory, volume 41 of Graduate Texts in Mathematics. Springer-Verlag, New York, second edition, 1990.

[2] Jane Arledge and David Grant. An explicit theorem of the square for hyperelliptic Jacobians. Michigan Math. J., 49(3):485–492, 2001.

[3] H. F. Baker. On the Hyperelliptic Sigma Functions. Amer. J. Math., 20(4):301–384, 1898.

[4] H. F. Baker. Introduction to the Theory of Multiply Periodic Functions. Cambridge University Press, 1907.

[5] H. F. Baker. Abelian functions. Cambridge Mathematical Library. Cambridge University Press, Cambridge, 1995. Abel's theorem and the allied theory of theta functions, Reprint of the 1897 original, With a foreword by Igor Krichever.

[6] Iacopo Barsotti. Considerazioni sulle funzioni theta. pages 247–277, 1970.

[7] Iacopo Barsotti. A new look for thetas. In Theta functions—Bowdoin 1987, Part 1 (Brunswick, ME, 1987), volume 49 of Proc. Sympos. Pure Math., pages 649–662. Amer. Math. Soc., Providence, RI, 1989.

[8] Christina Birkenhake and Herbert Lange. Complex abelian varieties, volume 302 of Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]. Springer-Verlag, Berlin, second edition, 2004.

[9] C. Blakestad and D. Grant. Universal p-adic sigma and weierstrass zeta functions. In preparation.

[10] Siegfried Bosch, Werner Lütkebohmert, and Michel Raynaud. Néron models, volume 21 of Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)]. Springer-Verlag, Berlin, 1990.

[11] Francesco Bottacin. Algebraic methods in the theory of theta functions. Ann. Scuola Norm. Sup. Pisa Cl. Sci. (4), 17(2):283–296, 1990.

[12] Lawrence Breen. Fonctions thêta et théorème du cube, volume 980 of Lecture Notes in Mathematics. Springer-Verlag, Berlin, 1983.

[13] Maurizio Candilera and Valentino Cristante. Bi-extensions associated to divisors on abelian varieties and theta functions. Ann. Scuola Norm. Sup. Pisa Cl. Sci. (4), 10(3):437–491, 1983.

[14] V. Cristante. Theta functions and Barsotti-Tate groups. Ann. Scuola Norm. Sup. Pisa Cl. Sci. (4), 7(2):181–215, 1980.

[15] Valentino Cristante. p-adic theta series with integral coefficients. Astérisque, (119-120):6, 169–182, 1984. p-adic cohomology.

[16] I. Dolgachev and D. Lehavi. On isogenous principally polarized abelian surfaces. In Curves and abelian varieties, volume 465 of Contemp. Math., pages 51–69. Amer. Math. Soc., Providence, RI, 2008.

[17] B. Edixhoven, G. van der Geer, and B. Moonen. Abelian Varieties. Book draft.

[18] L. Gerritzen. On non-Archimedean representations of abelian varieties. Math. Ann., 196:323–346, 1972.

[19] David Grant. Formal groups in genus two. J. Reine Angew. Math., 411:96–121, 1990.

[20] David Grant. Modular models of genus 2 curves and their Jacobians. In preparation.

[21] Robin Hartshorne. Algebraic geometry. Springer-Verlag, New York-Heidelberg, 1977. Graduate Texts in Mathematics, No. 52.

[22] Michiel Hazewinkel. Formal groups and applications. AMS Chelsea Publishing, Providence, RI, 2012. Corrected reprint of the 1978 original.

[23] Felix Klein. Ueber hyperelliptische Sigmafunctionen. Math. Ann., 27(3):431–464, 1886.

[24] Felix Klein. Ueber hyperelliptische Sigmafunctionen. Math. Ann., 32:357–387, 1888.

[25] Serge Lang. Elliptic functions, volume 112 of Graduate Texts in Mathematics. Springer-Verlag, New York, second edition, 1987. With an appendix by J. Tate.

[26] Qing Liu. Algebraic geometry and arithmetic curves, volume 6 of Oxford Graduate Texts in Mathematics. Oxford University Press, Oxford, 2002. Translated from the French by Reinie Erné, Oxford Science Publications.

[27] Ju. I. Manin. The Hasse-Witt matrix of an algebraic curve. Izv. Akad. Nauk SSSR Ser. Mat., 25:153–172, 1961.

[28] B. Mazur and J. Tate. Canonical height pairings via biextensions. In Arithmetic and geometry, Vol. I, volume 35 of Progr. Math., pages 195–237. Birkhäuser Boston, Boston, MA, 1983.

[29] B. Mazur and J. Tate. The p-adic sigma function. Duke Math. J., 62(3):663–688, 1991.

[30] B. Mazur, J. Tate, and J. Teitelbaum. On p-adic analogues of the conjectures of Birch and Swinnerton-Dyer. Invent. Math., 84(1):1–48, 1986.

[31] Barry Mazur. Rational points of abelian varieties with values in towers of number fields. Invent. Math., 18:183–266, 1972.

[32] Barry Mazur, William Stein, and John Tate. Computation of p-adic heights and log convergence. Doc. Math., (Extra Vol.):577–614, 2006.

[33] John Patrick McCabe. P-ADIC THETA-FUNCTIONS. ProQuest LLC, Ann Arbor, MI, 1968. Thesis (Ph.D.)–Harvard University.

[34] J. S. Milne. Abelian varieties. In Arithmetic geometry (Storrs, Conn., 1984), pages 103–150. Springer, New York, 1986.

[35] J. S. Milne. Jacobian varieties. In Arithmetic geometry (Storrs, Conn., 1984), pages 167–212. Springer, New York, 1986.

[36] Hisasi Morikawa. Theta functions and abelian varieties over valuation fields of rank one. I. Nagoya Math. J., 20:1–27, 1962.

[37] D. Mumford. On the equations defining abelian varieties. I. Invent. Math., 1:287–354, 1966.

[38] D. Mumford. On the equations defining abelian varieties. II. Invent. Math., 3:75–135, 1967.

[39] D. Mumford. On the equations defining abelian varieties. III. Invent. Math., 3:215–244, 1967.

[40] D. Mumford, J. Fogarty, and F. Kirwan. Geometric invariant theory, volume 34 of Ergebnisse der Mathematik und ihrer Grenzgebiete (2) [Results in Mathematics and Related Areas (2)]. Springer-Verlag, Berlin, third edition, 1994.

[41] David Mumford. Bi-extensions of formal groups. In Algebraic Geometry (Internat. Colloq., Tata Inst. Fund. Res., Bombay, 1968), pages 307–322. Oxford Univ. Press, London, 1969.

[42] David Mumford. The red book of varieties and schemes, volume 1358 of Lecture Notes in Mathematics. Springer-Verlag, Berlin, expanded edition, 1999. Includes the Michigan lectures (1974) on curves and their Jacobians, With contributions by Enrico Arbarello.

[43] David Mumford. Tata lectures on theta. I. Modern Birkhäuser Classics. Birkhäuser Boston, Inc., Boston, MA, 2007. With the collaboration of C. Musili, M. Nori, E. Previato and M. Stillman, Reprint of the 1983 edition.

[44] David Mumford. Tata lectures on theta. II. Modern Birkhäuser Classics. Birkhäuser Boston, Inc., Boston, MA, 2007. Jacobian theta functions and differential equations, With the collaboration of C. Musili, M. Nori, E. Previato, M. Stillman and H. Umemura, Reprint of the 1984 original.

[45] David Mumford. Tata lectures on theta. III. Modern Birkhäuser Classics. Birkhäuser Boston, Inc., Boston, MA, 2007. With collaboration of Madhav Nori and Peter Norman, Reprint of the 1991 original.

[46] David Mumford. Abelian varieties, volume 5 of Tata Institute of Fundamental Research Studies in Mathematics. Published for the Tata Institute of Fundamental Research, Bombay; by Hindustan Book Agency, New Delhi, 2008. With appendices by C. P. Ramanujam and Yuri Manin, Corrected reprint of the second (1974) edition.

[47] Peter Norman. p-adic theta functions. Amer. J. Math., 107(3):617–661, 1985.

[48] Peter Norman. Explicit p-adic theta functions. Invent. Math., 83(1):41–57, 1986.

[49] Peter Roquette. Analytic theory of elliptic functions over local fields. Hamburger Mathematische Einzelschriften (N.F.), Heft 1. Vandenhoeck & Ruprecht, Göttingen, 1970.

[50] Stephen S. Shatz. Group schemes, formal groups, and p-divisible groups. In Arithmetic geometry (Storrs, Conn., 1984), pages 29–78. Springer, New York, 1986.

[51] Joseph H. Silverman. Advanced topics in the arithmetic of elliptic curves, volume 151 of Graduate Texts in Mathematics. Springer-Verlag, New York, 1994.

[52] Joseph H. Silverman. The arithmetic of elliptic curves, volume 106 of Graduate Texts in Mathematics. Springer, Dordrecht, second edition, 2009.

[53] John Tate. A review of non-Archimedean elliptic functions. In Elliptic curves, modular forms, & Fermat's last theorem (Hong Kong, 1993), Ser. Number Theory, I, pages 162–184. Int. Press, Cambridge, MA, 1995.

[54] John Tate. Finite flat group schemes. In Modular forms and Fermat's last theorem (Boston, MA, 1995), pages 121–154. Springer, New York, 1997.

[55] José Felipe Voloch. An analogue of the Weierstrass ζ-function in characteristic p. Acta Arith., 79(1):1–6, 1997.